Oracle® Fusion Applications

Patching Guide

11*g* Release 1 (11.1.3)

E16602-14

March 2012

Documentation for installers and system administrators that describes how to use the patching framework tools to install, update and maintain Oracle Fusion Applications software between major releases.

ORACLE®

Oracle Fusion Applications Patching Guide, 11g Release 1 (11.1.3)

E16602-14

Primary Author: Vickie Laughlin

Contributors: Subash Chadalavada, Lori Coleman, Rick Lotero, Jay Lu, Prashant Salgaocar, Venkatesh Sangam, Praveena Vajja

Contents

3   Using Oracle Fusion Applications Patch Manager

4   Patching Oracle Fusion Applications Artifacts

5 Installing Release Update Patches (11.1.3.0.0)

6 Maintaining Oracle Fusion Applications Languages

7   Patching Oracle Fusion Middleware Extensions for Applications

8   Patching Oracle Fusion Functional Setup Manager

9   Patching Oracle Fusion Applications Functional Core

10 Performing System Maintenance Tasks

11 Monitoring and Troubleshooting Patches

A   Release Update Patch Installer Screens

B   Language Pack Installer Screens

x

Preface

This guide provides information about using the patching framework tools to update and maintain your Oracle Fusion Applications software between major releases.

Audience

This guide is intended for system administrators and patch administrators who are responsible for performing Oracle Fusion Applications patching tasks.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to 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.

Related Documents

For more information, see the following documents:

- *Oracle Fusion Applications Administrator and Implementor Roadmap*

- *Oracle Fusion Applications Concepts Guide*

- *Oracle Fusion Applications Administrator's Guide*

- *Oracle Fusion Applications Installation Guide*

- *Oracle Fusion Applications Enterprise Deployment Guide*

- *Oracle Fusion Middleware Concepts Guide*

- *Oracle Fusion Middleware Administrator's Guide*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's New in This Guide for Release 11.1.3

For Release 11.1.3, this guide has been updated in several ways. The following table lists the sections that have been added or changed.

Sections	Changes Made
Chapter 5 Installing Release Update Patches	
Section 5.1.4, "RUP Installer Configuration Tasks"	Section revised to add new configuration tasks
Section 5.2, "Prepare to Install a RUP - Pre-Down Time"	Section revised to add new prerequisites
Section 5.3, "Prepare to Install a RUP - During Downtime"	Section revised to add new prerequisites
Section 5.5, "Troubleshoot RUP Installer Sessions"	Section revised to add new troubleshooting sections
Chapter 6, Maintaining Oracle Fusion Applications Languages	
Section 6.1.5, "Language Pack Installer Configuration Tasks"	Section revised to add new configuration tasks
Section 6.2, "Prepare to Install a Language Pack Pre-Down Time"	Section revised to add new prerequisites
Section 6.3, "Prepare to Install a Language Pack - During Down Time"	Section revised to add new prerequisites
Section 6.4, "Install a Language Pack"	Section revised to add steps for Verifying Node Manager and OPMN Status
Section 6.5, "Troubleshooting Language Pack Installer Sessions"	Consolidated troubleshooting for both language packs and release update patches in Chapter 5.
Chapter 11, Monitoring and Troubleshooting Patches	
Section 11.3, "General Troubleshooting for Oracle Fusion Applications Patching"	Section revised to describe additional troubleshooting scenarios.
Appendix B, Language Pack Installer Screens	
Appendix B, "Language Pack Installer Screens"	New appendix

1

Introduction to Oracle Fusion Applications Patching Framework

The Oracle Fusion Applications patching framework provides the tools to support updates to Oracle Fusion Applications software. This chapter introduces the Oracle Fusion Applications patching framework and its components.

This chapter contains the following topics:

- Maintaining Oracle Fusion Applications
- Oracle Fusion Applications Patching Framework Components
- Oracle Fusion Applications Patching Framework Processes

1.1 Maintaining Oracle Fusion Applications

Oracle Fusion Applications is a deployment of applications product offerings built on the Oracle Fusion Middleware technology stack and Oracle Database. Each application artifact and the underlying Oracle Fusion middleware engine has its own development life cycle and patching requirements. The primary purpose of the Oracle Fusion Applications patching framework is to simplify and expedite the maintenance of the code and functionality shipped as part of Oracle Fusion Applications.

Even though a variety of middleware technologies is involved, the patching framework transparently uses multiple tools and utilities. The tools used to maintain Oracle Fusion Applications and its underlying components vary based on the type and requirements of the components.

Maintaining Oracle Fusion Applications

Oracle Fusion Applications requires various maintenance actions during its life cycle. Those actions impact the installed applications, their middleware dependencies, and their database components. Maintenance actions include applying patches to fix bugs, adding new functionality and features, installing a maintenance release, or providing interoperability to new technology stacks. Oracle Fusion Applications Patch Manager can be used to apply patches, while RUP Installer can be used to add functionality that is not delivered in individual patches.

Adding and Maintaining Languages

In addition to helping you maintain the Oracle Fusion Applications core functionality, the patching framework helps you add and maintain language content. The provisioning process installs the American (US) English language. When you want to add a different language after completing the installation process, you apply a language pack with Oracle Fusion Applications Language Pack Installer.

Maintaining Oracle Fusion Applications Patch Manager

When updates to Oracle Fusion Applications Patch Manager are available, you must use the OPatch utility to install these updates. For more information about OPatch, see the *Oracle Fusion Middleware Patching Guide*.

Maintaining Oracle Fusion Middleware Extensions for Applications

When updates to the Oracle home for Oracle Fusion Middleware Extensions for Applications are required, you use Oracle Fusion Applications AutoPatch to apply patches. For more information, see the applicable chapter:

- Chapter 7, "Patching Oracle Fusion Middleware Extensions for Applications"
- Chapter 8, "Patching Oracle Fusion Functional Setup Manager"
- Chapter 9, "Patching Oracle Fusion Applications Functional Core"

Maintaining Oracle Fusion Middleware Components

The Oracle Fusion Applications patching framework patches only the Oracle Fusion Applications content inside the Oracle Fusion Applications Oracle home. For more information, see Section 2.1.2, "Oracle Fusion Applications Oracle Home". When you must update middleware components, such as Oracle Enterprise Scheduler Service and Oracle WebLogic Service, use the OPatch utility. For more information, see the *Oracle Fusion Middleware Patching Guide*.

1.2 Oracle Fusion Applications Patching Framework Components

The Oracle Fusion Applications patching framework provides the following components, tools, and utilities to maintain and update Oracle Fusion Applications.

1.2.1 Oracle Fusion Applications Patch Manager

The primary function of Oracle Fusion Applications Patch Manager is to manage patches that update both the database and middleware artifacts under the Oracle Fusion Applications Oracle home. It calls the Oracle Fusion Applications AutoPatch utility to patch database artifacts and the OPatch utility to coordinate activities for updating middleware artifacts. For conceptual information about Oracle Fusion Applications Patch Manager, see Chapter 2, "Understanding Oracle Fusion Applications Patching Concepts". For information about how to use this product, see Chapter 3, "Using Oracle Fusion Applications Patch Manager".

1.2.2 Oracle Fusion Applications Release Update Patch Installer

Release Update Patch Installer allows you to install Release Update Patches to update your version of Oracle Fusion Applications. For more information, see Chapter 5, "Installing Release Update Patches (11.1.3.0.0)".

1.2.3 Oracle Fusion Applications Language Pack Installer

Language Pack Installer allows you to add languages at any time after the initial provisioning and installation of Oracle Fusion Applications. For more information, see Chapter 6, "Maintaining Oracle Fusion Applications Languages".

1.2.4 AD Administration

The AD Administration utility performs maintenance tasks that keep applications files and database objects current. For more information, see Chapter 10, "Performing System Maintenance Tasks".

1.2.5 AD Controller

The AD Controller utility helps you troubleshoot database tasks performed by Oracle Fusion Applications Patch Manager or AD Administration and allows you to control their actions. For more information, see Section 11.5, "Troubleshooting Patching Sessions for Database Content".

1.2.6 HomeChecker

The HomeChecker utility verifies the correctness of any Oracle Fusion Applications Oracle home directory. For more information, see Section 10.5, "Running the HomeChecker Utility".

1.3 Oracle Fusion Applications Patching Framework Processes

The high-level processes related to patching Oracle Fusion Applications are outlined in Table 1–1, along with links to chapters in this guide that contain the detailed instructions.

Table 1–1   Oracle Fusion Applications Patching Processes

Process	Description	Link to Documentation
Apply patches and run reports	Run Oracle Fusion Applications Patch Manager	Chapter 3, "Using Oracle Fusion Applications Patch Manager"
Deploy artifacts	Perform required deployments steps for specific artifacts	Chapter 4, "Patching Oracle Fusion Applications Artifacts"
Install release update patches	Run Release Update Patch Installer	Chapter 5, "Installing Release Update Patches (11.1.3.0.0)"
Maintain languages	Install language packs and apply language patches	Chapter 6, "Maintaining Oracle Fusion Applications Languages"
Maintain Oracle Fusion Middleware Extensions for Applications	Run Oracle Fusion Applications AutoPatch	Chapter 7, "Patching Oracle Fusion Middleware Extensions for Applications"
Maintain Oracle Fusion Functional Setup Manager	Run Oracle Fusion Applications AutoPatch	Chapter 8, "Patching Oracle Fusion Functional Setup Manager"
Maintain Oracle Fusion Applications Functional Core	Run Oracle Fusion Applications AutoPatch	Chapter 9, "Patching Oracle Fusion Applications Functional Core"
Run maintenance tasks	Run AD Administration	Chapter 10, "Performing System Maintenance Tasks"
Monitor, verify, and troubleshoot the application of patches	Monitor Oracle Fusion Applications Patch Manage sessions and resolve any reported issues	Chapter 11, "Monitoring and Troubleshooting Patches"

2

Understanding Oracle Fusion Applications Patching Concepts

This chapter describes concepts that you should understand before you use the Oracle Fusion Applications patching framework.

This chapter contains the following topics:

- Patching Topology and Configuration
- Patch Types
- Patch Directory Structure and Contents
- Oracle Fusion Applications Patching and the Security Model

2.1 Patching Topology and Configuration

Provisioning a new Oracle Fusion Applications environment begins with a choice of the applications product offerings you intend to install and continues through configuring and deploying the applications. The patching framework must *know* about the configuration of the offerings and their middleware and database components to identify the artifacts and servers that are affected during patch application. The patching software is installed and configured with other system components during the provisioning process.

See "Applications Topology — Oracle WebLogic Server Domains" in the *Oracle Fusion Applications Installation Guide* for more information about installing, configuring, and deploying applications.

This section contains the following topics related to patching topology and configuration:

- Patching Installation and Configuration
- Oracle Fusion Applications Oracle Home
- Patch Top Directory
- Backup Copies of Patched Database Artifacts
- Oracle Universal Installer (OUI) Inventory
- Taxonomy URL

2.1.1 Patching Installation and Configuration

The provisioning process installs the artifacts required by patching. Then the process calls the patching configuration utility to configure the patching framework for the Oracle Fusion Applications system, as follows:

- Populates a properties file in the `admin` directory, `FUSION_env.properties`, that contains complete environment setup information required by the patching framework. This is the source of information that patching framework utilities use when setting up the environment for patching.

- Creates the patching framework configuration scripts that set the environment and call utilities. For example, it creates the script, `fapmgr.sh` in UNIX (`fapmgr.cmd` in Windows), which sets up the environment and then calls Oracle Fusion Applications Patch Manager.

2.1.2 Oracle Fusion Applications Oracle Home

The patching framework and the Oracle Fusion Applications software are installed into what is known as the *Oracle Fusion Applications Oracle home*. This Oracle home directory, `/net/oracle/fusionapps/applications`, is a subdirectory under the Oracle Fusion Applications Middleware home. There is one and only one set of patching-related software and database tables for each Oracle home. Figure 2–1 shows the related directory structure.

> **Note:** Unless otherwise specified, the usage of "Oracle home" and *FA_ORACLE_HOME* in this guide refers to the Oracle Fusion Applications Oracle home.

Figure 2–1   Oracle Fusion Applications Directory Structure
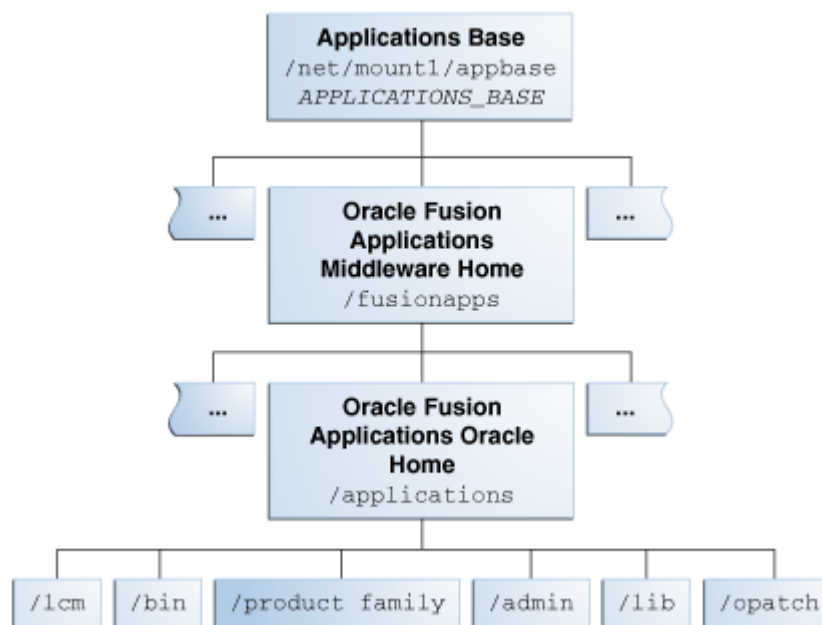
The Oracle home contains the following subdirectories:

- **lcm**: Contains the patching framework software in the following subdirectories:

- – `.../ad/bin`: Patching framework software and files, including C artifacts and configuration scripts that set the environment and start the corresponding utility

  – `.../ad/java`: Java artifacts

  – `.../ad/db/sql`: Database artifacts and SQL files

  – `.../ad/lib`: Application libraries

  – `.../ad/template`: Configuration files or templates delivered and used by the patching framework during configuration activities

- **bin**: Contains applications artifacts called by Enterprise Scheduler Service jobs.

- *product family*: Contains directories for artifacts specific to a product configuration.

- **admin**: Contains the patching framework environment properties file (`FUSION_env.properties`), Oracle Fusion Applications AutoPatch and the patching logs, reports, and administration files. These files are required by Oracle Fusion Applications Patch Manager.

- **lib**: Contains applications-specific libraries.

- **OPatch**: Contains the OPatch utility called by Oracle Fusion Applications Patch Manager when patching middleware artifacts. This version of OPatch is used to apply patches to the middleware files and software artifacts that reside within the Oracle Fusion Applications Oracle home, `.../net/oracle/fusionapps/applications`, and is delivered as part of the Oracle Fusion Applications software. Note that you may have multiple versions of OPatch to support your enterprise software.

For more information about the components that are part of this directory structure, see "Provisioned Oracle Fusion Applications Home Directories" in the *Oracle Fusion Applications Administrator's Guide*.

2.1.3 Patch Top Directory

The patch top directory is any directory you select for downloading patch ZIP files. You unzip the patches in this directory and refer to this directory path as needed when applying patches. This directory is also called `patch_top` or `PATCH_TOP`. For example, if you download patch 1234567.zip into `/home/mypatches` and unzip it there, the patch top directory is `/home/mypatches/1234567`.

2.1.4 Backup Copies of Patched Database Artifacts

When applying a patch that includes a later version of an existing database artifact in the Oracle home, Oracle Fusion Applications Patch Manager automatically backs up the existing database artifacts being replaced into a backup directory. The default location for the backup directory is `admin/pbackup` under the Oracle home. If needed, you can override this location by editing the `PATCH_BACKUP_DIR` parameter in the `FUSION_env.properties` file.

2.1.5 Oracle Universal Installer (OUI) Inventory

The Oracle Universal Installer inventory stores information about all Oracle software products and components installed in all Oracle homes. Each product, such as Oracle Fusion Applications, maintains its own local inventory and Oracle home. Local inventory files for Oracle Fusion Applications exist in the Oracle Fusion Applications

Oracle home and the patching framework reads and updates these files. Each Oracle home contains OUI components. In Oracle Fusion Applications, each product family is assigned an OUI component and other entities are also assigned a component. For example, the component `oracle.fusionapps.fin` is assigned to Oracle Fusion Financials. The patching framework uses this information to identify and determine the specific contents of the patch that are applicable to the Oracle home and to perform patch validation, patch verification, and reporting. The location of the OUI Inventory directory, can be found at `/etc/oraInst.loc` (UNIX) or `C:\Program Files\Oracle\Inventory` (Windows).

For more information, see "Oracle Universal Installer Inventory" in the *Oracle Universal Installer and OPatch User's Guide*.

2.1.6 Taxonomy URL

Oracle Fusion Applications Patch Manager queries the taxonomy mbean URL as defined by the environment property called `taxonomy_url` in order to determine which domains a specific patch impacts, such as where a Java EE application is running or where a Service-Oriented Architecture (SOA) composite is deployed. The URL points to an Administration Server of the domain where taxonomy MBeans are hosted. This variable is set during the provisioning process in the `FUSION_env.properties` file. You can override this value during patching by providing the `taxonomyurl` option when running Oracle Fusion Applications Patch Manager. For example, if the server being referenced by the default `taxonomy_url` is down, you can enter an overriding URL from the command line.

2.2 Patch Types

Oracle Fusion Applications patches typically contain one or more bug fixes. A *bug fix* is associated with a bug number, which is used by Oracle development to track fixes to the software. A *patch* is a delivery vehicle for releasing bug fixes to customers.

On occasion, patches may contain new features, test and diagnostic scripts, and additional documentation. For example, a standard patch focuses on solving specific issues and is applied using Oracle Fusion Applications Patch Manager, while a language pack is applied with Oracle Fusion Applications Language Pack Installer and contains the translated content required to add a language other than English. The *patch type* describes the way the patch is packaged and applied. Patches are released in the types shown in Table 2–1.

Table 2–1   Patch Types

Format	Description	Utility Used
Standard Patch	A patch delivered to solve one or more customer issues. It may contain multiple bug fixes within a product family and includes the high-watermark of all related files or software artifacts included in the patch.	Oracle Fusion Applications Patch Manager
One-Off Patch	A patch containing a single bug fix for specific artifacts. It is created on an exception basis at the request of a customer for an issue that affects only that customer.	Oracle Fusion Applications Patch Manager
Language Pack	Translation content for a language other than English for the entire Oracle Fusion Applications suite, for a base release.	Language Pack Installer

Table 2–1   (Cont.) Patch Types

Format	Description	Utility Used
Release Update Patch	A set of cumulative patches for the entire Oracle Fusion Applications Suite.	Release Update Patch Installer

2.2.1 Impact of a One-off Patch

Oracle may provide a one-off patch in order to fix a customer specific issue. A one-off patch is different from a standard patch because it contains only a single bug fix for each artifact included in the patch. A standard patch includes the high water mark of changes for the artifacts included in the patch.

A one-off patch is applied on an exception basis. After the one-off patch is delivered, Oracle provides a standard patch that includes the same fix as the one-off patch. When the standard patch is available, it replaces the one-off patch and should be applied to your environment as soon as possible.

> **Note:**   After you apply a one-off patch for a middleware artifact, your environment contains versions of artifacts that will conflict with any subsequent standard patch for that same component. Oracle Fusion Applications Patch Manager prevents any new standard patches from being applied by setting a lock for that component. For example, after you apply a one-off patch for a database artifact, a lock is set for that artifact. To remove this lock, you must apply the standard patch to supersede the one-off patch. This standard patch delivers the same fix as the one-off patch, and also includes the high water mark for related artifacts.

2.3 Patch Directory Structure and Contents

Oracle Fusion Applications patches often include content for both middleware artifacts and database artifacts. The patching framework examines the high-level contents of each patch and calls the appropriate patching tool to process the patch content.

2.3.1 Patch Directory Structure

Using patch number 123456 as an example of a patch that contains both database and middleware artifacts, the unzipped patch directory, *PATCH_TOP*/123456, contains the files and subdirectories shown in Figure 2–2. If a patch contains only database artifacts or only middleware artifacts, the `123456_MW` directory and `123456_DB` directory do not exist, respectively.

Figure 2–2 Example of the Directory Structure of a Patch
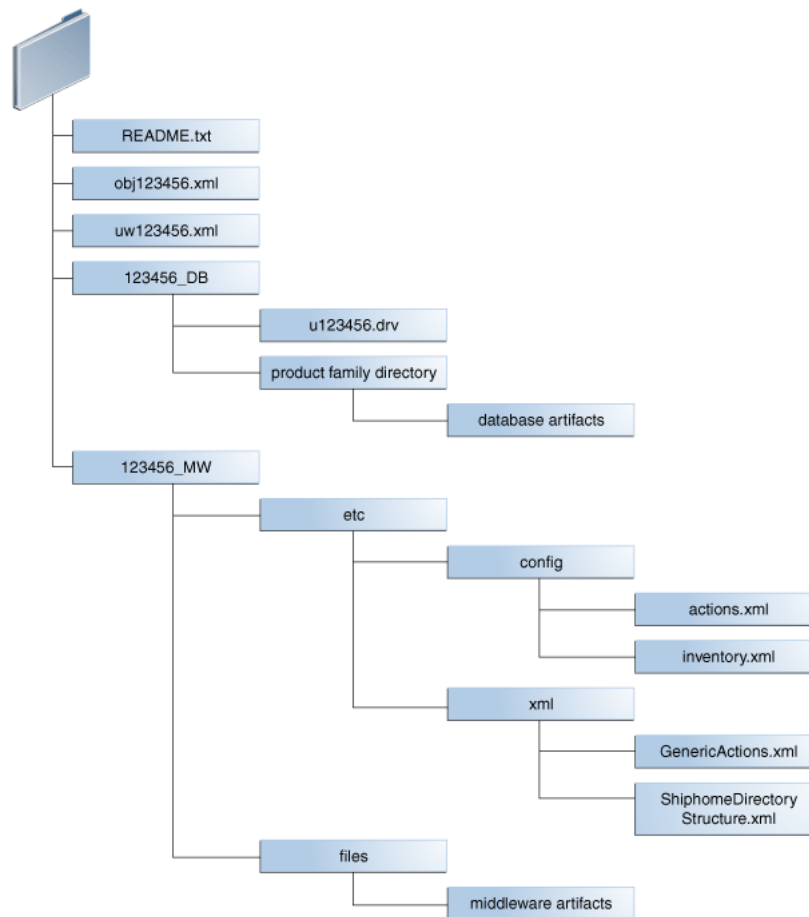
2.3.2 Patch Contents

Sample patch contents follow, using patch number 123456 as an example of a patch that contains both database and middleware artifacts:.

- `README.txt`: Provides general instructions for applying the patch and for performing manual steps, if required by the patch. If there are patches listed under "Other Patches" in the README file, you must download and apply them before you apply the Oracle Fusion Applications patch.

- `obj123456.xml`: Contains information about each artifact included in the patch.

  An example of the contents of the `obj123456.xml` file follows.

```
<?xml version="1.0" encoding="UTF-8"?>

<PATCH_OBJECT_MANIFEST VERSION="1.0">
 <COMPONENT TYPE="MW">
   <OBJECT_INFO NAME="AdfPjgTopPublicUi.jar"
SUBDIR="prj/deploy/EARProjectsFinancials.ear/EARProjectsFinancials/WEB-INF/lib"
SRCDIR="prj/deploy/EARProjectsFinancials.ear/EARProjectsFinancials/WEB-INF/lib"
PRODUCTFAMILY="prj" PRODUCT="pjg" LBA="PjgTop"
APPNAME="EARProjectsFinancials.ear"
HEADERSTRING="$AppsHeader:fusionapps/prj/components/projectsFinancials/jlib/Adf
PjgTopPublicUi.jar st_fusionapps_pt/63 level:0 00.S $"

OUI_COMPONENT="oracle.fusionapps.prj.deploy" VERSION="63.0" TRANSLATION_
```

```
LEVEL="0" ACTION="COPY" ARTIFACT_TYPE="JEE" />
 </COMPONENT>
        <COMPONENT TYPE="DB">
                <OBJECT_INFO NAME="pjf_event_type_data.sql"
SUBDIR="prj/pjf/db/sql"
SRCDIR="prj/pjf/db/sql" PRODUCTFAMILY="prj" PRODUCT="pjf"
LBA="" APPNAME="" HEADERSTRING="$Header: fusionapps/prj/pjf/db/sql/pjf_event_
type_data.sql"
OUI_COMPONENT="oracle.fusionapps.prj.db" VERSION="st_fusionapp/1"
TRANSLATION_LEVEL="0" />
        </COMPONENT>
        <COMPONENT TYPE="DB">
                <OBJECT_INFO NAME="pjf_event_type_data.sql"
SUBDIR="prj/pjf/db/sql"
PRODUCTFAMILY="prj" PRODUCT="pjf" LBA="" APPNAME=""
HEADERSTRING="$Header: fusionapps/prj/pjf/db/sql/pjf_event_type_data.sql"
OUI_COMPONENT="oracle.fusionapps.prj.db" VERSION="st_fusionapps/1"
TRANSLATION_LEVEL="0" />
        </COMPONENT>
</PATCH_OBJECT_MANIFEST>
```

- uw123456.xml: Contains high-level information about the patch and provides the following information.

    - Translation and platform attributes

    - Prerequisite patches

    - Additional bug fixes that are included in the patch

    - Compatibility information for the patch such as product family and application name

    - Type of patch content and attributes, such as the patch driver location and whether manual steps exist

An example of the contents of the uw123456.xml file follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<!--PATCHGEN_VERSION:    11.1.1.5.0-->
<!--OPACK_LABEL:         /net/sta.world.com/OPATCH_MAIN_
GENERIC.rdd/opatch/OPack-->
<!--OPACK_VERSION:       null-->
<!--VIEW_LABEL:          FUSIONAPPS_PT.2000.S-->
<!--PATCH_COMMAND:       ant stFullPatchTransaction -Dtransaction=prj_adflib_
db -Dinclude=ALL -Dbugid=123456 -->
<PatchManifest Version="1.0">
<PatchList PatchType="SNOWBALL" Translatable="Y" PartialTranslations="N"
HighAvailability="DERIVE" Merge="N" GUID="1004567" >
        <Patch Number="123456" Language="US" Platform="GENERIC" GUID="1004567"
BaseBug="123456" BaseProductFamily="UNKNOWN" BaseProduct="UNKNOWN" BaseLBA=""
Description="" />
</PatchList>
<PreReqBugfixList>
</PreReqBugfixList>
<RequiredComponentList>
        <RequiredComponent ID="oracle.fusionapps.prj.deploy"
Version="11.1.1.5.0" />
        <RequiredComponent ID="oracle.fusionapps.prj.db" Version="11.1.1.5.0" />
</RequiredComponentList>
<BugfixList>
        <Bugfix Number="123456" ProductFamily="" Product="" LBA=""
Description=""/>
```

```
</BugfixList>
<Impact>
        <ProductFamilyList>
                <ProductFamily Name="prj">
                <ProductList>
                        <Product Name="pjf">
                        </Product>
                        <Product Name="pjg">
                        <LBAList>
                                <LBA Name="PjgTop"/>
                        </LBAList>
                        </Product>
                </ProductList>
                </ProductFamily>
        </ProductFamilyList>
        <ApplicationList>
                <Application Name="EARProjectsFinancials.ear"/>
        </ApplicationList>
</Impact>
<ContentList>
                        </Product>
                        <Product Name="pjg">
                        <LBAList>
                                <LBA Name="PjgTop"/>
                        </LBAList>
                        </Product>
                </ProductList>
                </ProductFamily>
        </ProductFamilyList>
        <ApplicationList>
                <Application Name="EARProjectsFinancials.ear"/>
        </ApplicationList>
</Impact>
<ContentList>
        <Content Type="DB" PreApplySteps="N" PostApplySteps="N"
PatchDriver="u123456.drv"
PatchDriverLocation="123456_DB" DataModelChanges="N" SeedDataChanges="N"
PlSqlChanges="N" SQLChanges="Y" FlexChanges="N" LDAPChanges="N"
DataSecurityChanges="N" />
        <Content Type="MW" PreApplySteps="N" PostApplySteps="N"
PatchDriverLocation="123456_MW" />
</ContentList>
</PatchManifest>
```

- `123456_DB`: Contains files related to changes for the database artifacts included in this patch, bundled so that they can be accessed and applied using Oracle Fusion Applications AutoPatch.

  The following files exist in the `123456_DB` directory:

  - `u123456.drv`: Contains instructions for Oracle Fusion Application AutoPatch to make changes to an Oracle Fusion Applications database and is referred to as the patch driver file.

  - Product family directory: Contains the patch content for database artifacts in a form that is readable by Oracle Fusion Applications AutoPatch.

- `123456_MW`: Contains files related to middleware artifact changes included in this patch, bundled so that they can be accessed and applied using OPatch. The patch content resides under the `files` subdirectory in a form that is readable by OPatch. The patch metadata resides under the `etc` subdirectory.

The middleware metadata files exist in the following subdirectories:

– `etc/config/actions.xml`

An example of the contents of the `actions.xml` file follows:

```
<oneoff_actions>
    <oracle.fusionapps.prj.deploy version="11.1.1.5.0" opt_req="R">
        <copy name="AdfPjgTopPublicUi.jar" path="%ORACLE_
HOME%/prj/deploy/EARProjectsFinancials.ear/EARProjectsFinancials/WEB-INF/li
b" file_name="prj/deploy
/EARProjectsFinancials.ear/EARProjectsFinancials/WEB-INF/lib/AdfPjgTopPubli
c
Ui.jar" file_version="63.0"/>
    </oracle.fusionapps.prj.deploy>
</oneoff_actions>
```

– `/etc/config/automation.xml`

An example of the contents of the `automation.xml` file follows:

```
<automation xmlns="http://oracle.com/schema/opatch/Automation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://oracle.com/schema
/opatch/Automation ../../xsd/automation.xsd" opatch-version="11.1.0.6.0"
deployment-type="fapps" deployment-sub-type="fapps-artifacts">
    <post-patch-application>
        <deploy-action acts-on="SOAComposite">
            <deploy-artifact file-name="sca_
FinGlCurrencyUserPreferredCurrencyComposite.jar"
 destination-path="%ORACLE_HOME%/fin/deploy" name="FinGlCurrencyUser
PreferredCurrencyComposite" revision="7_5512345"/>
        </deploy-action>
    </post-patch-application>
</automation>
```

– `/etc/config/checksum.xml`

An example of the contents of the `checksum.xml` file follows:

```
checksum_info>
    <file path="%ORACLE_HOME%/fscm/security/policies/system-jazn-data.xml"
checksum="-1"/>
</checksum_info>
```

– `etc/config/inventory.xml`

An example of the contents of the `inventory.xml` file follows:

```
<oneoff_inventory>
    <opack_version version="11.1.0.6.0"/>
    <patch_id number="123456"/>
    <cannot_autorollback>false</cannot_autorollback>
    <date_of_patch year="2011" month="Feb" day="16" time="10:47:37 hrs"
zone="PST8PDT"/>
    <base_bugs>
        <bug number="123456" description="fusionapps patch"/>
    </base_bugs>
    <required_components>
        <component internal_name="oracle.fusionapps.prj.deploy"
version="11.1.1.5.0" opt_req="R"/>
    </required_components>
    <os_platforms>
        <platform name="Generic Platform 2" id="2000"/>
```

```
                    </os_platforms>
                    <executables></executables>
                    <instance_shutdown>false</instance_shutdown>
                    <instance_shutdown_message></instance_shutdown_message>
                    <online_rac_installable>false</online_rac_installable>
                    <run_as_root>false</run_as_root>
                    <sql_migrate>false</sql_migrate>
                    <wls_prereq_oneoffs></wls_prereq_oneoffs>
                    <os_platforms>
                        <platform name="Generic Platform 2" id="2000"/>
                    </os_platforms>
                    <executables></executables>
                    <instance_shutdown>false</instance_shutdown>
                    <instance_shutdown_message></instance_shutdown_message>
                    <online_rac_installable>false</online_rac_installable>
                    <run_as_root>false</run_as_root>
                    <sql_migrate>false</sql_migrate>
                    <wls_prereq_oneoffs></wls_prereq_oneoffs>
                    <prereq_oneoffs></prereq_oneoffs>
                    <coreq_oneoffs></coreq_oneoffs>
                    <overlay_oneoffs></overlay_oneoffs>
                    <patch_type value="snowball"/>
                    <patch_language value="en"/>
                    <product_family value="fusionapps"/>
                    <patching_model value="snowball"/>
                    <auto>false</auto>
                    <translatable>true</translatable>
                    <applicable_product/>
                    <products></products>
                    <update_components></update_components>
                </oneoff_inventory>
```

2.4 Oracle Fusion Applications Patching and the Security Model

In Oracle Fusion Applications, credentials used for patching are stored securely, based in the Lightweight Directory Access Protocol (LDAP) Credential Store Framework (CSF), where they can be retrieved when required and hidden when starting processes from the command line. Credentials are not stored in any format, in the file system or in the database. Users are not prompted for passwords when using command-line utilities. A separate role is not used for patching purposes because all patch administrators log in as the same operating system user to apply patches. This user must be an owner of the Oracle Fusion Applications Oracle home.

For more information, see the *Oracle Fusion Middleware Application Security Guide*.

Obtaining Credentials

Oracle Fusion Applications Patch Manager obtains passwords from the CSF based on the following:

- CSF APIs are used to obtain passwords from the CSF.

- A combination of a MAP and a KEY returns the user name, and its corresponding password, in decrypted format.

All credentials are securely stored in a wallet that is stored in LDAP. Oracle Fusion Applications Patch Manager credentials are available under the oracle.patching MAP name and each credential is identified by a KEY.

Using CSF APIs

The patching framework uses CSF APIs to retrieve credentials. It does not pass the credentials at the command line when calling either Oracle Fusion Applications AutoPatch or OPatch.

No Password Prompts in Interactive Mode

Security can be breached when you are prompted for a password while invoking patching from the command line. To avoid this situation, Oracle Fusion Applications Patch Manager uses the Oracle Platform Security Services APIs to fetch passwords from the CSF.

Removing Credentials from Files

Oracle Fusion Applications Patch Manager uses a defaults file to store the arguments and other information required for a given session, but does not read or write credentials to or from the defaults file. Likewise, Oracle Fusion Applications Patch Manager does not read or write credentials from restart files or log files.

3

Using Oracle Fusion Applications Patch Manager

This chapter describes how to use the features of Oracle Fusion Applications Patch Manager.

This chapter contains the following topics:

- Introduction to Oracle Fusion Applications Patch Manager
- Running Oracle Fusion Applications Patch Manager
- Validating Patches
- Applying Patches
- Running Patching Reports
- End-to-End Process for Applying Individual Patches
- End-to-End Process for Applying Multiple Patches

3.1 Introduction to Oracle Fusion Applications Patch Manager

The primary function of Oracle Fusion Applications Patch Manager is to apply standard and one-off patches. It can also validate whether patches can be applied and generate patching reports.

Oracle Fusion Applications Patch Manager provides a command-line interface to coordinate its patching functions. A single patch may include changes to both middleware and database artifacts, and these middleware artifacts may be deployed to Managed Servers running on different nodes. The artifacts are updated in the Oracle Fusion Applications Oracle home that is shared by the different nodes. To patch both types of artifacts, two patching tools are called by Oracle Fusion Applications Patch Manager to manage the actions involved: *OPatch* for the middleware artifacts and *Oracle Fusion Applications AutoPatch* for artifacts associated with the database. Both Oracle Fusion Applications AutoPatch and OPatch have long been used as the standard patching tools in previous releases of Oracle products.

The same set of patching-related software and database tables is used by both Oracle Fusion Applications Patch Manager and Oracle Fusion Middleware Extensions for Applications (Applications Core). Oracle Fusion Applications Patch Manager and Applications Core each reside in their own separate Oracle home and use their specific shell scripts to support their product-specific patching requirements. These scripts are uniquely defined to reference the appropriate Oracle home, set the patching configuration and environment, and then call the Oracle Fusion Applications

AutoPatch utility for database patching. There can be only one patching session active for Oracle Fusion Applications or Applications Core at a time.

For more information about patching Applications Core, see Chapter 7, "Patching Oracle Fusion Middleware Extensions for Applications".

The following topics provide additional information about Oracle Fusion Applications Patch Manager:

- Coordinated Patching
- Patching Middleware Artifacts
- Patching Database Artifacts
- Online and Offline Patching
- Applying Multiple Patches Using a My Oracle Support Patch Plan

3.1.1 Coordinated Patching

Oracle Fusion Applications Patch Manager examines patch metadata and determines which actions must be performed by OPatch and which must be performed by Oracle Fusion Applications AutoPatch. If Oracle Fusion Applications Patch Manager discovers that a patch contains only database changes, it assigns the patch directly to Oracle Fusion Applications AutoPatch for processing. If the patch is related only to middleware changes, Oracle Fusion Applications Patch Manager orchestrates the application of the changes across domains and the Oracle home. If the patch contains both database and middleware changes, Oracle Fusion Applications Patch Manager coordinates the application of both changes, applying database changes first, followed by middleware changes. You apply the patch in a single operation, regardless of the type of artifacts that are updated.

Figure 3–1 illustrates the patching process coordinated by Oracle Fusion Applications Patch Manager.

Figure 3–1   Oracle Fusion Applications Coordinated Patching
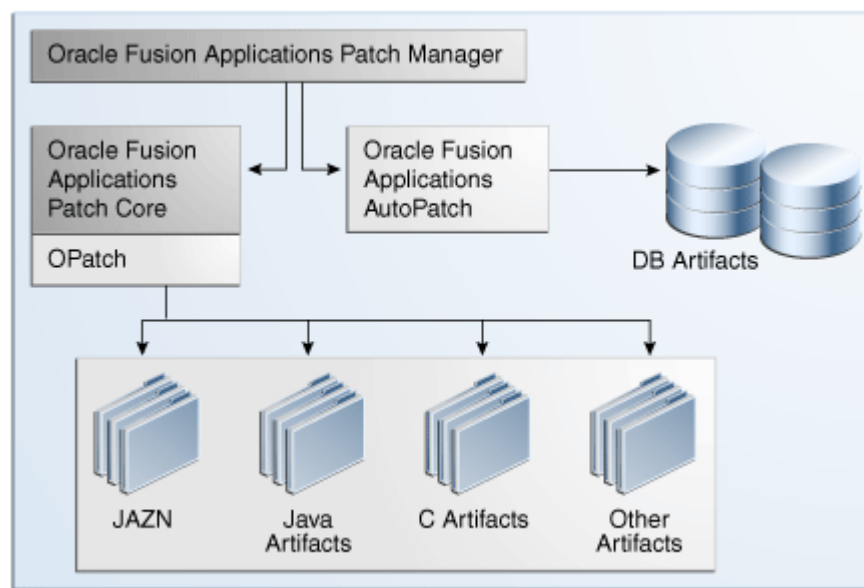
Example of Patch Coordination

The following high-level phases occur when you apply a patch in online mode that contains an Oracle Application Development Framework (Oracle ADF) library and a seed data file for a product family:

- Oracle Fusion Applications Patch Manager interprets the contents of the patch by reading the patch metadata.

- Oracle Fusion Applications AutoPatch updates the seed data.

- OPatch applies the change to the Oracle ADF library in the form of a JAR file.

- Oracle Fusion Applications Patch Manager coordinates with OPatch and forces an immediate shutdown and restart of the impacted Managed Servers so the change to the Oracle ADF library takes effect.

- Oracle Fusion Applications Patch Manager consolidates and provides results and status for the overall patching tasks in the Log Summary and the Diagnostics report.

3.1.2 Patching Database Artifacts

When a patch contains updates to database artifacts, such as application seed data, the database schema, PL/SQL objects, and SQL scripts, Oracle Fusion Applications Patch Manager calls Oracle Fusion Applications AutoPatch to coordinate the following tasks:

- **Worker calculation:** Calculates the default number of workers that should be used. If patching is run on the same machine as the database server, the default number of workers is calculated as 0.5 times the number of VCPUs on the database server. If patching is run on a machine different from the database server on a Linux platform, the default number of workers is calculated as the minimum of the VCPUs available on the database server and the patching machine. On non-Linux platforms, the default number of workers is equal to the number of VCPUs on the database server. You must reduce the number of workers if the machine where you are applying the patch has a lower number of VCPUs when compared to those on the database server. To override the default number of workers when you apply a patch, specify the number of workers by using the `workers` option, as described in Table 3–3. To override the default number of workers when you install a release update patch, specify the number of workers by using the `-J-Dworkers` option, as described in Table 5–3.

  The number of workers used for patching database artifacts also imposes a requirement on the open file descriptors configured for your system. Patching requires that the open file descriptors be set to a minimum of 8000 times the number of workers used for the patch session. For more information, see "Increase the Open Files Limit" in the *Oracle Fusion Applications Installation Guide*.

  For more information about workers, see Section 3.1.2.1, "Worker Processes".

- **Patch validation:** Validates whether the database portion of the patch is compatible with your environment and can be applied. If the patch is not valid, the patching session fails. The following validations are performed:

  - Platform check: Compares the operating system platform for each Oracle Fusion Applications Oracle home against the platform metadata in the patch.

  - Prerequisite check: Validates that all patch prerequisites have been applied.

- **Application of the patch:** Copies the database artifacts to the Oracle home and then makes changes in the Oracle Fusion Applications database using the updated files.

- **Compilation of invalid objects:** Compiles all invalid objects in the database. For more information, see Section 3.1.2.3, "Compiling Invalid Objects".

- **Consolidation of log files:** Collects the patching outcome and location of log files for reporting purposes.

A patch with database-related changes includes a patch driver file that provides instructions to Oracle Fusion Applications AutoPatch about how to apply the patch. The patch driver file specifies the types of actions to be executed and the phases in which they must be executed. To achieve efficient processing time, the database tasks are performed by worker processes and the number of tasks performed is minimized by file version verification. For more information, see Section 3.1.2.1, "Worker Processes" and Section 3.1.2.2, "File Version Verification".

3.1.2.1 Worker Processes

An Oracle Fusion Applications AutoPatch *manager* process reads the patch driver file and determines the set of tasks to be performed. It then spawns processes called *workers* to execute the tasks. The manager and its workers communicate through a table in the database that contains one row for each worker process. The manager assigns tasks to workers by updating the worker row in the table. Each worker process checks the table for updates to its row and carries out the task. When the task is complete, the worker updates the status in the table, and the manager then assigns another task to the worker.

3.1.2.2 File Version Verification

This Oracle Fusion Applications AutoPatch feature enables incremental running of database-related actions in a patch so that only the actions that have not already been performed against your database are actually run. The first time a database update action runs, the version of the file used to update the database is recorded in tables in the applications database. The next time Oracle Fusion Applications AutoPatch applies a patch containing that action, it compares the version of the last file run against the current version of the file in the patch. It runs the action only if the version in the patch is newer than the last version run.

3.1.2.3 Compiling Invalid Objects

Oracle Fusion Applications Patch Manager uses the standard database-supplied compile utility, which compiles all invalid objects in the database, if no specific schema is supplied. If a schema is supplied it compiles all objects in the schema that are in an invalid state, including those invalid objects that were not affected by the patch. Dependencies between objects can be complex, such as when patching an object causes other objects to become invalid, even though those objects are not in the patch. The purpose of compiling invalid objects is to have a clean database where all objects are in a valid state.

3.1.3 Patching Middleware Artifacts

The middleware artifacts may be deployed to Managed Servers running on different nodes, but the artifacts are copied to the Oracle Fusion Applications Oracle home that is shared by the different nodes. When a patch contains updates to middleware artifacts, such as Java EE applications or Service-Oriented Architecture (SOA) composites, Oracle Fusion Applications Patch Manager coordinates the following tasks during online patching:

- Patch preparation: Sets up credentials and other necessary environment variables.

- Patch validation: Validates the patch against the patch inventory under the Oracle home and domain to ensure that the patch is compatible and the prerequisite patches can be applied.

- Topology discovery: Queries the taxonomy tables to find information relevant to the artifacts contained in the patch, such as domains, hosts, the Administration Server URL and Oracle homes. If the query returns exceptions, patching may proceed or fail, depending on the artifact type.

- Application of the patch: Calls OPatch to copy the middleware artifacts from the patch to the Oracle Fusion Applications Oracle home. Also deploys those artifacts to the appropriate run-time container so that they are usable, such as deploying a SOA composite to the appropriate SOA server. Note that all artifacts in the patch are copied, but deployment actions occur only for those product families that have been deployed during the provisioning process. Finally, tracks the success or failure of each patching action and performs validation as needed, based on the directives specified in the patch metadata.

- Post-patch apply actions: Starts and stops the Managed Servers impacted by the patch in the respective domains, only in online mode. Performs the deployment of certain middleware artifacts.

- Consolidation of log files: Collects the patch results and location of log files for reporting purposes.

For more information, see Table 4–1, " Oracle Fusion Middleware Artifacts Supported by Oracle Fusion Applications Patch Manager".

3.1.4 Online and Offline Patching

Oracle Fusion Applications Patch Manager supports two patching modes: *online* and *offline*. To apply any patch in online mode, the Administration Servers must be running. For both offline and online modes, the database is still running, but it should be idle. Oracle WebLogic Server is not connected to the database for performing any transactions, so no requests from users should be processed. As the patch administrator, it is your responsibility to ensure that there are no active transactions or processes running during patching.

3.1.4.1 Online Mode

The primary difference between online and offline modes is that in online mode, Oracle Fusion Applications Patch Manager automates the post-apply steps, such as shutting down and starting the impacted Managed Servers, and deploying supported middleware artifacts, such as SOA composites, Oracle Business Intelligence Publisher (Oracle BIP) artifacts, and Flexfields. For more information, see Section 4.1, "Oracle Fusion Applications Patch Manager Middleware Artifact Support". When patching in online mode, Oracle Fusion Applications Patch Manager provides messages about the steps you must take after the patch is applied, to resolve any failures that occurred during the post-apply tasks.

To enable online patching mode, you specify the `online` option when you run Oracle Fusion Applications Patch Manager. Oracle Fusion Applications Patch Manager determines which domains the patch affects by referencing the taxonomy URL, either by an environment setting or by using the `taxonomyurl` option. For more information, see Section 2.1.6, "Taxonomy URL".

Note that this automation feature attempts to stop and start only those impacted servers that are running. No stop or start operations are performed on those servers that are not in a running state even if the patch impacts an application that is deployed

on this server. During online patching, all servers and applications are running, but they must be idle. Applications login should be restricted and no Oracle Fusion Applications functions should be available to users during online patching. If you prefer to start and stop your Managed Servers using your own process, you can apply online patches in offline mode.

3.1.4.2 Offline Mode

You must manually start and stop the impacted Managed Servers and manually deploy certain middleware artifacts, such as SOA composites, Oracle BI Publisher artifacts, and Flexfields, after you apply patches in offline patching mode. You can run the Patch Impact report to see which servers will be impacted by the patch. For information about server management for offline patching, see "Starting and Stopping a Product Family Oracle WebLogic Server Domain" in the *Oracle Fusion Applications Administrator's Guide*.

To minimize downtime, you could choose to leave servers running and start and stop the servers impacted by the patches after the patching session ends. In offline mode, all applications are unavailable to users, but only the servers impacted by the patch must be shut down. The net effect is that the system is unavailable, but the system downtime is minimized if only certain servers are shut down and then started.

3.1.5 Applying Multiple Patches Using a My Oracle Support Patch Plan

If you use the *Patch Plan* feature in My Oracle Support, you have the option to apply all of the patches in the patch plan during one Oracle Fusion Applications Patch Manager session. You can also validate these patches in one session. Depending on the contents of the patches, Oracle Fusion Applications Patch Manager processes the patches either one at a time or in a single execution. Applying the group of patches in a single execution minimizes down time because any impacted Managed Servers are stopped and restarted only once.

A set of patches can be applied in a single execution, rather than individually, only if servers can be shutdown at the beginning of the apply session and none of the included patches require the servers to be available. Therefore, true multiple patch application in online mode occurs only if the patches involved contain the following artifacts.

- Applications Policies (using the `system-jazn-data.xml` file)
- Oracle Business Intelligence Publisher (BI Publisher) artifacts
- Oracle Business Process Management (Oracle BPM) templates
- C artifacts
- Common Resource artifacts
- Database artifacts other than flexfields
- Diagnostic Testing Framework (DTF) JAR files
- Java EE artifacts
- Oracle Data Integrator (ODI) artifacts
- SOAEXTENSION artifacts

If any of the patches in the patch plan contains any other artifact types, then Oracle Fusion Applications Patch Manager applies each patch in the plan sequentially, one patch at a time, because certain servers must be running to deploy certain artifacts. In

this case, the server shutdown and restart occurs multiple times, as required by each patch.

For more information about patch plans, see the online help in the **Patches & Updates** tab in My Oracle Support.

3.2 Running Oracle Fusion Applications Patch Manager

You run Oracle Fusion Applications Patch Manager by using the command line utility, `fapmgr`, located in the *FA_ORACLE_HOME*/lcm/ad/bin directory (*FA_ORACLE_HOME*\lcm\ad\bin for Windows). Its shell script sets the environment and calls the utility. For UNIX, the shell script is `fapmgr.sh` and for Windows, it is `fapmgr.cmd`. You can run `fapmgr` with various commands and options. Only one patching session can be running at any given time. All patch administrators log in as the same operating system user to apply patches. This user must be an owner of the Oracle Fusion Applications Oracle home.

The following command shows the basic syntax for the `fapmgr` utility:

```
(UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh command [-options]
(Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd command [-options]
```

In the preceding example, the following variables are used:

- command: The `fapmgr` utility manages patching-related activities by using one of the commands as described in Table 3–1.

- options: The `fapmgr` commands accept options by using command-line arguments, as described in the following sections for each `fapmgr` command.

Table 3–1   Oracle Fusion Applications Patch Manager Commands

Command	Description and Link to Documentation
validate	Reads the actions in the patch metadata to determine whether a patch is compatible with your environment and can be applied. See Section 3.3, "Validating Patches".
apply	Applies a patch. See Section 3.4, "Applying Patches".
report	Provides options for generating reports related to patching. See Section 3.5, "Running Patching Reports".
retry	Provides the ability to retry post-apply tasks that failed. See Section 11.3.4, "Retrying Failed Post-Patching Tasks in a Previous Session".
bootstrap	Updates the Oracle Fusion Applications Patch Manager data model. See Section 4.15, "Patching Oracle Fusion Applications Patch Manager Artifacts".
abort	Abandons the previous patching session that failed. See Section 11.3.2, "Abandoning a Failed Patching Session".
forcefail	Forces a previously hung session to fail. See Section 11.3.3, "Recovering from an Interrupted Patching Session".

To view additional information for any `fapmgr` command, use the following syntax:

```
(UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh command -help
(Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd command -help
```

To display basic help for the `fapmgr` command, enter `fapmgr` with no options.

> **Note:** You must use a version of OPatch that is compatible with
> Oracle Fusion Applications when you run Oracle Fusion Applications
> Patch Manager. For more information, see Section 5.2.5, "Verify Your
> OPatch Version".

3.3 Validating Patches

The `fapmgr validate` command reads the actions in the patch driver file to
determine whether a patch is compatible with your environment and can be applied
successfully. It looks for the status of impacted servers, patch conflicts, and
prerequisites, but it does not perform any updates. Validation can be performed in
both offline and online modes.

Oracle Fusion Applications Patch Manager automatically performs patch validation
when you run the `fapmgr apply` command. The steps for validating a patch are
provided here because Oracle recommends that you validate every patch before
applying it, especially those patches that contain updates to SOA composites. You can
reduce downtime and potential failures during patching by validating SOA composite
patches because you can resolve validation issues before you apply the patch. For
more information about resolving these issues, see Section 11.4.2, "Troubleshooting
SOA Composite Validation Failures".

Validation performs the following actions:

- Checks if prerequisite patches have been applied

- Checks whether required taxonomy details can be successfully retrieved

- Checks whether the servers that are required for automated deployment of the
  middleware artifacts in the patch are running

- Checks whether a middleware artifact will be copied based on version checking

- Checks for patch conflicts

Syntax

Use the following syntax for the `validate` command:

```
(UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh validate -patchtop (or grouptop)
patchtop_directory \
[-patchingplan path_to_patch_plan_xml_file][-online] [-taxonomyurl
hostname:portnumber]
[-logfile log_file_name][-loglevel log level]

(Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd validate -patchtop (or grouptop)
patchtop_directory \
[-patchingplan path_to_patch_plan_xml_file][-online] [-taxonomyurl
hostname:portnumber]
[-logfile log_file_name] [-loglevel log level]
```

Options

Table 3–2 lists the options available for the `validate` command.

Table 3–2   validate Command Options

Option	Description	Mandatory
`patchtop`	Identifies the directory where the patch is unzipped	Yes, unless applying patches in a patch plan

Table 3–2   (Cont.) validate Command Options

Option	Description	Mandatory
grouptop	Identifies the directory where the patches in a patch plan are unzipped	Yes, when applying patches in a patch plan
patchingplan	Identifies the directory path to the My Oracle Support patch plan XML file	Yes, when applying patches in a patch plan
online	Validates patch in online mode so the status of impacted servers is checked.	No, default value is not online.
taxonomyurl	Identifies the host name and port number that overrides the default taxonomy information stored in the environment properties file. The Administration Server passes this value to Oracle Fusion Applications Patch Manager.	Conditionally required only when you want override the value present in the environment properties file and when using the online option.
logfile	Overrides the default log file name and sends the processing information to the file you specify, under the *FA_ORACLE_ HOME*/admin/FUSION/log directory. If you enter an existing file name, the output is appended to the file.	No, the utility generates a log file under *FA_ORACLE_ HOME*/admin/FUSION/log using this naming convention: FAPatchManager_validate_ *timestamp*.log
loglevel	Records messages in the log file at the level you specify. Enter a value to override the default log level of INFO. See Section 11.1, "Oracle Fusion Applications Patch Manager Logging".	No, default value is INFO.
help	Displays help.	No.

3.4 Applying Patches

You apply patches to an Oracle Fusion Applications environment by running the fapmgr apply command. Only one patching session can be active at a time.

Syntax

Use the following syntax for the apply command:

```
(UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh apply -patchtop (or grouptop) path_to_
unzipped_patch [-patchingplan path_to_XML_file] \
[-stoponerror] [-online][-taxonomyurl hostname:portnumber] \
[-workers number_of_database_workers] \
[-logfile log_file_name] [-loglevel level]

(Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd apply -patchtop (or grouptop path_
to_unzipped_patch [-patchingplan path_to_XML_file]\
[-stoponerror] [-online] [-taxonomyurl hostname:portnumber] \
[-workers number_of_database_workers] \
[-logfile log_file_name] [-loglevel level]
```

Example

The following example applies a patch using 10 database workers in online mode:

```
(UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh apply -patchtop path_to_unzipped_patch
-stoponerror -online -workers 10

(Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd apply -patchtop path_to_unzipped_
patch \
-stoponerror -online -workers 10
```

Options

Table 3–3 lists the options available for the `apply` command.

Table 3–3   apply Command Options

Option	Description	Mandatory
`patchtop`	Identifies the directory where the patch is unzipped.	Yes, when applying an individual patch.
`grouptop`	Identifies the directory where the patches in a patch plan are unzipped	Yes, when applying patches in a patch plan
`patchingplan`	Identifies the directory path to the My Oracle Support patch plan XML file	Yes, when applying patches in a patch plan
`stoponerror`	Patching session fails after a post-apply error is reported. You can then manually resolve the issue and start the session again, using the same command.	Yes, when patching in online mode.
`workers`	Identifies the number of workers to use when running database tasks. If you provide a value for the number of workers that is outside the calculated range, you are prompted to provide a value that is within the optimal range. If you do not use the `workers` option, a calculated optimal value is used.	No, default value is calculated if patch contains database tasks. See "Worker Calculation" in Section 3.1.2, "Patching Database Artifacts".
`online`	Applies patch in online mode so that impacted servers are shut down and started and supported artifacts are deployed. See Section 3.1.4, "Online and Offline Patching".	No, default value is not online. Use this option only when applying online patches.
`taxonomyurl`	Identifies the host name and port number that overrides the default taxonomy information stored in the environment properties file. The Administration Server passes this value to Oracle Fusion Applications Patch Manager.	Conditionally required only when you want to override the value present in the environment properties file and when using the online option.
`logfile`	Overrides the default log file name and sends the processing information to the file you specify, under the `FA_ORACLE_HOME`/`admin`/`FUSION`/`log` directory. If you enter an existing file name, the output is appended to the file.	No, the utility generates a log file under `FA_ORACLE_HOME`/`admin`/`FUSION`/`log` using this naming convention: `FAPatchManager_apply_timestamp.log`
`loglevel`	Records messages in the log file at the level you specify. Enter a value to override the default log level of `INFO`. See Section 11.1, "Oracle Fusion Applications Patch Manager Logging".	No, default value is `INFO`.
`help`	Displays help.	No.

3.5 Running Patching Reports

You can generate Oracle Fusion Applications Patch Manager reports by running the `fapmgr report` command. You can view patch-related information from different perspectives to plan your patching strategy. These reports provide information that can be useful both before and after you apply patches.

Table 3–4 describes the patching reports that can be generated by Oracle Fusion Applications Patch Manager.

Table 3–4   Patching Reports

Report Name	Report Option	Description	Variations
Patch Impact Report	-patchimpact	Displays the impact of a patch in terms of bug fixes, prerequisites, and product families, by displaying what exists on your system. Also provides a list of artifact types, along with related servers and required manual actions.	None.
Product Families Report	-listcomps	Displays a list of installed components (product families) and their versions.	You can specify a list of product families or you can see all product families.
Patches Applied Report	-listpatches	Displays information about patches and bug fixes that have been applied to your system.	You can specify a list of product families or you can see all product families.
Patch Status Report	-isapplied	Tells you whether specific patches or bug fixes were applied to your system.	None.
Diagnostics Report	-patchprogress	Displays the progress of a patching session that is currently running.	This report runs automatically after each patching session. You can also run it during a patching session.

The fapmgr report command requires an option to specify which report you want to run, followed by mandatory and optional parameters.

Use the following syntax to run a report:

```
(UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh report -report_option -mandatory
parameters \
[optional parameters]

(Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd report -report_option -mandatory
parameters \
[optional parameters]
```

3.5.1 Patch Impact Report

The Patch Impact report compares the contents of the patch to be applied with the files that currently exist on your system. You get a complete picture of what file system changes will occur when you apply the patch. You can plan your system downtime by viewing the servers that will be impacted by the patch, along with any manual deployment actions that are required after the patch applies. This report reads the patch metadata, local patch inventory, and the current view snapshot. For more information, see Section 10.2, "Maintaining Snapshot Information". Note that you cannot run the Patch Impact report when you are applying multiple patches that were download in a patch plan.

The Patch Impact report displays the impact information about a patch in five sections: bug fixes, prerequisite bug fixes, impacted product families, servers impacted, and files included in the patch.

Bug Fixes

This section provides the following information about the bug fixes included in the patch:

- Bug Number: The number of the bug fix or patch

- Bug Description: The description of the bug fix or patch

- Exists in Oracle home: Whether the bug fix or patch was already applied (Yes or No)

Prerequisite Bug Fixes

This section provides the following information about patches that must be applied before the current patch can be applied:

- Bug Number: The number of the prerequisite bug fix or patch

- Bug Description: The description of the prerequisite bug fix or patch

- Exists in Oracle home: Whether the prerequisite bug fix or patch was already applied (Yes or No)

Prerequisite Bug Fixes Not In FA_ORACLE_HOME

This section provides the following information about patches that must be applied before the current patch can be applied. These patches are not applied to FA_ORACLE_HOME.

- Bug Number: The number of the prerequisite bug fix or patch

- Bug Description: The description of the prerequisite bug fix or patch

- Exists in Oracle home: Whether the prerequisite bug fix or patch was already applied (No)

Product Families Impacted

This section provides the following information about which product families are impacted by the patch:

- Product Family: The name of the product family (component) that is updated by the patch

- Product: The name of the product that is updated by the patch

- LBA: The logical business area that is updated by the patch

Servers Impacted

This section provides the following information about which servers will be impacted by the patch. Note that all artifacts in the patch are copied, but server life cycle actions occur only for those product families that have been deployed during the provisioning process.

- Artifact Type: The type and name of the artifact included in the patch

- Domain (Servers): The servers that are impacted by the artifacts in the patch

- Expectation/Impact: The description of what servers must be running, what actions will be taken during the patch apply phase by Oracle Fusion Applications Patch Manager, and what manual actions must be taken

Files Included in the Patch

This section provides the following information about the files that are included in the patch:

- File Name: The name of the file

- File Type: The type of the file

- File Version: The version of the file

3.5.1.1 Running the Patch Impact Report

Before you run the Patch Impact report, ensure that the snapshot is current for the environment. For more information, see Section 10.2, "Maintaining Snapshot Information". Note that you cannot run the Patch Impact report when you are applying multiple patches that were download in a patch plan.

Use the following syntax to run the Patch Impact report:

```
(UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh report -patchimpact -patchtop  \
 path_to_unzipped_patch [optional parameters]

(Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd report -patchimpact -patchtop  \
path_to_unzipped_patch [optional parameters]
```

The following table describes the parameters used by the Patch Impact report.

Parameter	Mandatory	Description
patchtop	Yes	Identifies the directory where the patch is unzipped.
outputfile	No	Sends the report output to the file you specify after this parameter. You cannot use an existing file name. If you do not use this parameter, no output file is created.
logfile	No	Overrides the default log file name and sends the processing information to the file you specify, under the *FA_ORACLE_HOME*/admin/FUSION/log directory. If you enter an existing file name, the output is appended to the file. If you do not use this parameter, the utility generates a log file under *FA_ORACLE_HOME*/admin/FUSION/log using this naming convention: FAPatchManager_report-patchimpact_*timestamp*.log
loglevel	No	Records messages in the log file at the level you specify. Enter a value to override the default log level of INFO. See Section 11.1, "Oracle Fusion Applications Patch Manager Logging".
reportwidth	No	Sets the column width to either 80 columns or 132 columns by specifying NORMAL or WIDE. The default value is 80 columns, or NORMAL.

3.5.2 Product Families Report

The Product Families report provides a list of installed product families along with each associated Oracle Universal Installer (OUI) component name and version. You can run the report for all product families or you can select specific product families. This report reads the local patch inventory and the current view snapshot.

The report includes the following information:

- OUI Component: Component name assigned to the product family

- Version: The version of the product family

- Product Family: The product family name

- Description: The product family description

3.5.2.1 Running the Product Families Report

Before you run the Product Families report, ensure that the snapshot is current for the environment. For more information, see Section 10.2, "Maintaining Snapshot Information".

Use the following syntax to run the Product Families report:

```
(UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh report -listcomps [optional parameters]
```

```
(Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd report -listcomps [optional
parameters]
```

The following table describes the parameters used by the Product Families report.

Parameter	Mandatory	Description
comps	No	Supply a comma-separated list of product families (components) you want to see on the report. The report includes all product families if you do not use this parameter.
outputfile	No	Sends the report output to the file you specify after this parameter. You cannot use an existing file name. If you do not use this parameter, no output file is created.
logfile	No	Overrides the default log file name and sends the processing information to the file you specify, under the FA_ORACLE_HOME/admin/FUSION/log directory. If you enter an existing file name, the output is appended to the file. If you do not use this parameter, the utility generates a log file under FA_ORACLE_HOME/admin/FUSION/log using this naming convention: FAPatchManager_report-listcomps_timestamp.log
loglevel	No	Records messages in the log file at the level you specify. Enter a value to override the default log level of INFO. See Section 11.1, "Oracle Fusion Applications Patch Manager Logging".
reportwidth	No	Sets the column width to either 80 columns or 132 columns by specifying NORMAL or WIDE. The default value is 80 columns, or NORMAL.

3.5.2.2 Example Syntax for the Product Families Report

Examples of the command syntax for running the Product Families report follow:

How to show all installed product families and their versions
```
(UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh report -listcomps
(Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd report -listcomps
```

How to show specific product families and specify the report output file name and log file name
```
(UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh report -listcomps -comps
```

```
oracle.fusionapps.crm, oracle.fusionapps.fin \
-outputfile listproducts.txt -logfile /log/listproducts.log

(Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd report -listcomps -comps
oracle.fusionapps.crm, oracle.fusionapps.fin \
-outputfile listproducts.txt -logfile \log\listproducts.log
```

3.5.3 Patches Applied Report

The Patches Applied report provides information about patches that have been applied to an environment. You can run the report for specific product families or all product families. This report depends on a current snapshot having been run.

The report is organized by product family (OUI component) and each product family section contains the following information:

- Patch Number: The patch number

- Patch Type: Possible values are Standard or ONE-OFF

- Date Applied: The date the patch was applied

- Bugs Fixed: The bug fixes included in each patch that was applied

3.5.3.1 Running the Patches Applied Report

Before you run the Patches Applied report, ensure that the snapshot is current for the environment. For more information, see Section 10.2, "Maintaining Snapshot Information".

Use the following syntax to run the Patches Applied report:

```
(UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh report -listpatches [optional
parameters]

(Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd report -listpatches [optional
parameters]
```

The following table describes the parameters used by the Patches Applied report.

Parameter	Mandatory	Description
comps	No	Supply a comma-separated list of product families you want to see on the report. The report includes all product families if you do not use this parameter.
outputfile	No	Sends the report output to the file you specify after this parameter. You cannot use an existing file name. If you do not use this parameter, no output file is created.
logfile	No	Overrides the default log file name and sends the processing information to the file you specify, under the FA_ORACLE_HOME/admin/FUSION/log directory. If you enter an existing file name, the output is appended to the file. If you do not use this parameter, the utility generates a log file under FA_ORACLE_HOME/admin/FUSION/log using this naming convention: FAPatchManager_report-listpatches_timestamp.log
loglevel	No	Records messages in the log file at the level you specify. Enter a value to override the default log level of INFO. See Section 11.1, "Oracle Fusion Applications Patch Manager Logging".

Parameter	Mandatory	Description
reportwidth	No	Sets the column width to either 80 columns or 132 columns by specifying NORMAL or WIDE. The default value is 80 columns, or NORMAL.

3.5.3.2 Example Syntax for the Patches Applied Report

Examples of the command syntax for running the Patches Applied report follow:

How to show all patches applied and set the report width to 132

```
(UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh report -listpatches -reportwidth WIDE

(Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd report -listpatches -reportwidth
WIDE
```

How to show all patches applied for a list of product families

```
(UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh report -listpatches -comps
oracle.fusionapps.fin, oracle.fusionapps.crm
(Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd report -listpatches -comps
oracle.fusionapps.fin, oracle.fusionapps.crm
```

3.5.4 Patch Status Report

The Patch Status report tells you if specific patches or bug fixes have been applied to an environment. You provide a list of patch numbers or bug fixes when you run the report and the output indicates whether each patch or bug fix has been applied. This report queries the local patch inventory and current view snapshot. For more information, see Section 10.2, "Maintaining Snapshot Information".

The report output contains a table with the following columns:

- Bug Number: The bug number.

- OUI Component: Component name associated with the product family. This column displays "Not Applied" if the patch was not applied.

- Status: Possible values are Applied and Not Applied.

- Patch: The patch number. This column displays Not Applied if the patch was not applied.

- Date Applied: The date the patch was applied. This column is null if the patch was not applied.

3.5.4.1 Running the Patch Status Report

Use the following syntax to run the Patch Status report:

```
(UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh report -isapplied -bug or -patch\
[comma-separated_list_of_patches/bug_fixes [optional parameters]

(Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd report -isapplied -bug or -patch \
comma-separated_list_of_patches/bug_fixes [optional parameters]
```

The following table describes parameters used by the Patch Status report.

Parameter	Mandatory	Description
`bug`	Yes, unless the `patch` parameter is used.	Supply a comma-separated list of bug fixes. If you want to request language bug fixes, append the language code to the bug number, for example, `123456:KO`.
`patch`	Yes, unless the `bug` parameter is used.	Supply a comma-separated list of patches. If you want to request language patches, append the language code to the patch number, for example, `123456:KO`.
`outputfile`	No	Sends the report output to the file you specify after this parameter. You cannot use an existing file name. If you do not use this parameter, no output file is created.
`logfile`	No	Overrides the default log file name and sends the processing information to the file you specify, under the `FA_ORACLE_HOME`/admin/FUSION/log directory. If you enter an existing file name, the output is appended to the file. If you do not use this parameter, the utility generates a log file under `FA_ORACLE_HOME`/admin/FUSION/log using this naming convention: `FAPatchManager_report-listpatches_timestamp.log`
`loglevel`	No	Records messages in the log file at the level you specify. Enter a value to override the default log level of `INFO`. See Section 11.1, "Oracle Fusion Applications Patch Manager Logging".
`reportwidth`	No	Sets the column width to either 80 columns or 132 columns by specifying `NORMAL` or `WIDE`. The default value is 80 columns, or `NORMAL`.

3.5.5 Diagnostics Report

After each patching sessions ends, the Diagnostics report is automatically generated so that you can view the results of the session. You can also use this report to monitor a patching session that is currently running, by generating the report from the command line. The report output is in HTML format so that it can be viewed from a browser and is located in the `FA_ORACLE_HOME`/admin/FUSION/log/fapatch/fapatch_ 11.1.3.0.0 directory. You can refresh the report output as the patch progresses.

The Diagnostics report contains three sections.

Module Execution Summary

The Module Execution Summary displays high-level information about the tools used during a patching session, such as Oracle Fusion Applications Patch Manager, OPatch, and Oracle Fusion Applications AutoPatch. For each tool, the report displays the following information:

- Module: Tool called during the patching session, such as Oracle Fusion Applications Patch Manager

- Status: Completion status of the task, such as Success, Failed, or Skipped

- Duration: Total time that the module ran

- Start Time: Time and date the module started

- End Time: Time and date the module ended

- Log Files: Link to the Log Summary generated by Oracle Fusion Applications Patch Manager. For more information, see Section 11.2.1, "Log Summary".

Module Phase Summary

The Module Phase Summary displays summary information about tasks executed by Oracle Fusion Applications Patch Manager. The tasks are summarized by each AutoPatch and OPatch phase and the following information is displayed:

- Mode: The patching mode is either Database or Middleware

- Phase: The name of the patching phase

- Duration: Total time the task ran

- Start Time: Time and date the task started

- End Time: Time and date the task ended

- Task Count: Total number of tasks within the phase

- Skipped: The number of tasks that were skipped during the phase

- Failed: The number of tasks that failed during the phase

- Completed: The number of tasks that completed successfully during the phase

- Percent Complete: The percentage of tasks that completed successfully during the phase

Module Task Details

The Module Task Details section displays detailed information about each task executed by Oracle Fusion Applications Patch Manager. The following information is displayed for each task:

- Mode: The patching mode is Database, Middleware, or Generic. In Generic mode, database validation and taxonomy URL validation are performed.

- Phase: The name of the patching phase, such as Patch Validation, Environment Validation, and Patch Application.

- Product Family: The short name of the product family, which displays only for database tasks.

- Task: The name of the artifact related to the task including the version, the full path, and the domain, if applicable.

- Status: Completion status of the task, such as Success, Failed, or Skipped.

- Duration: Total time the task ran.

- Start Time: Time and date the task started.

- End Time: Time and date the task ended.

- Warning/Error Message: The error message is displayed if the task failed. Nonfatal messages appear as warning messages. The message also includes additional steps that are required to resolve the failure, if applicable.

- Log File: The name and location of the log file.

- Line Number: The line numbers within the log file that pertain to the task.

Tasks to be Completed

The Tasks to be Completed section displays a summary of the tasks you must complete after the patch applies. The following information is displayed:

- Mode: The patching mode is Database, Middleware, or Generic. In Generic mode, database validation and taxonomy URL validation are performed.

- Phase: The name of the patching phase, such as Patch Validation, Environment Validation, and Patch Application

- Product Family: The short name of the product family, which displays only for database tasks.

- Task: The description of the task that must be performed.

3.5.5.1 Running the Diagnostics Report

Use the following syntax to run the Diagnostics report while a patch session is active:

```
(UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh report -patchprogress [optional
parameters]
```

```
(Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd report -patchprogress [optional
parameters]
```

The following table describes the parameter used by the Diagnostics report.

Parameter	Mandatory	Description
reportlocation	No	Supply with the full directory path and name of the report output. The default value is *FA_ORACLE_HOME*/admin/FUSION/log/FAPMgrDiagnosticsSummarydate:*fapmgr_commandtimestamp*.html.

3.6 End-to-End Process for Applying Individual Patches

The end-to-end process of obtaining and applying individual patches using Oracle Fusion Applications Patch Manager, includes the following steps. This process assumes that you apply patches in online mode. If you are applying patches in a patch plan, see Section 3.7, "End-to-End Process for Applying Multiple Patches".

> **Note:** As part of the patching process, customers have their own backup and recovery management process. Oracle recommends that you always have a current backup before applying a patch.

Step 1 Research Issue that Needs to be Resolved by a Patch

When you have an issue that needs to be resolved by a patch for Oracle Fusion Applications, file a service request with Oracle Support Services or research the issue on My Oracle Support:

```
http://support.oracle.com
```

Step 2 Check for Existing Patches

After you find patches that may resolve your issues, you should confirm whether you previously applied them to your system. Select one of these options for finding whether patches were applied:

- Run the Patch Status report to see if specific patches were applied, as described in Section 3.5.4, "Patch Status Report".

- Run the Patches Applied report to see all patches applied for a specific product family, as described in Section 3.5.3, "Patches Applied Report".

Step 3 Obtain and Unzip the Patches

Upon determining that you need new patches, download the patches from My Oracle Support. Unzip the patch ZIP files in your PATCH_TOP directory.

Step 4 Read the README File

Read the README file that accompanies each patch. This file contains important information and instructions that must be followed. If a patch contains preinstallation or postinstallation manual steps, they are described in the patch README file. If there are patches listed under "Other Patches" in the README file, you must download and apply them before you apply the Oracle Fusion Applications patch.

Step 5 Run the Patch Impact Report

Run the Patch Impact report to see the artifacts and Managed Servers impacted by this patch. For more information, see Section 3.5.1, "Patch Impact Report".

An example of the report command follows:

```
(UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh report -patchimpact -patchtop path_to_
unzipped_patch
```

```
(Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd report -patchimpact -patchtop path_
to_unzipped_patch
```

Step 6 Validate the Patch

Run the fapmgr validate command to alert you to any potential issues that could result in failure while applying the patch. You should resolve all validation failures during this step, to prevent failures during patch application. This validation step is strongly recommended, especially for patches that deliver artifacts whose deployment is automated by Oracle Fusion Applications Patch Manager, such as SOA composites. Note that if you validate a patch that contains BI Publisher artifacts, the BI OPMN control process, which is similar to a node manager, has to be up for online mode validation to succeed.

When you apply a patch, the patch validation runs again by default. For more information, see Section 3.3, "Validating Patches".

An example of the validate command follows:

```
(UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh validate -patchtop path_to_unzipped_
patch -online
(Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd validate -patchtop path_to_
unzipped_patch -online
```

Step 7 Prepare the System

To prevent locks on patched objects and other data issues during patching of database artifacts, review and perform the following checklist before patching the target environment:

1. Confirm that the database is running and in an idle state.

2. Confirm that there are no active jobs or processes running against the database. If there are, stop all background jobs, including jobs in the database and active processes

3. Confirm that the Managed Servers are not in "Edit and Lock" mode, so that Oracle Fusion Applications Patch Manager can stop and start servers as needed.

4. Manually shut down the Oracle Enterprise Scheduler Service (ESS) servers, especially when a patch contains a PL/SQL package, by performing the following steps:

   a. Stop the ESS request processor and dispatcher to prevent new requests from being processed. See "Starting and Stopping a Request Processor or Dispatcher" in the *Oracle Fusion Applications Administrator's Guide* for more information.

   b. Cancel any in-progress requests. See "Cancelling Oracle Enterprise Scheduling Service Job Requests" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Enterprise Scheduling Service* for more information.

   c. Shutdown the ESS WebLogic Server Managed server. See the "Starting and Stopping" table, specifically the "Managed Server for an application" row, in the *Oracle Fusion Applications Administrator's Guide* for more information.

5. If the patch contains BI Publisher reports, ensure that you have your own versions of any customized BI Publisher reports. If a patch includes an update to a catalog object that was delivered with an Oracle Fusion application, the patch will overwrite any customizations applied to the original report. For more information, see "Before You Begin Customizing Reports" in the Oracle Fusion Applications Extensibility Guide.

6. If the patch contains BI Publisher artifacts, the BI OPMN control process, which is similar to a node manager, has to be up for online mode validation to succeed.

7. This step is for the Windows operating system only. Ensure that there are no active files. If the lock is not released `fapmgr` will not be able to copy files.

Step 8 Apply the Patch

Apply the patch using the `fapmgr apply` command as described in Section 3.4, "Applying Patches". An example of the `apply` command follows:

```
(UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh apply -patchtop path_to_unzipped patch
\
-stoponerror -online [-workers number_of_database_workers]

(Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd apply -patchtop path_to_unzipped
patch \
-stoponerror -online [-workers number_of_database_workers]
```

Step 9 Monitor and Verify the Application of the Patch

Monitor the progress of the patching session and verify its successful completion by reviewing the Log Summary from a browser. For more information, see Section 11.2, "Monitoring Patching Sessions".

Step 10 Verify the Deployment of Middleware Artifacts

Review the Diagnostics report to determine if any artifacts require manual deployment or Managed Servers require restart. For example, this report displays the full path of SOA composites that restarted successfully and those that did not restart successfully, which requires additional manual steps. If any servers must be restarted manually, the report provides the target domain and the names of the cluster and Managed Servers that must be restarted. For more information, see Section 3.5.5, "Diagnostics Report".

You can manually perform these steps or you can use the `fapmgr retry` command. For more information, see Section 11.3.4, "Retrying Failed Post-Patching Tasks in a Previous Session".

For additional information about the deployment of middleware artifacts, see Section 4.1, "Oracle Fusion Applications Patch Manager Middleware Artifact Support".

3.7 End-to-End Process for Applying Multiple Patches

The end-to-end process of obtaining and applying multiple patches using Oracle Fusion Applications Patch Manager, assumes that you create and download a patch plan from My Oracle Support and you apply these patches in online mode. A set of patches can be applied in one execution, rather than individually, only if servers can be shutdown at the beginning of the apply session and none of the included patches require the servers to be available. See Section 3.1.5, "Applying Multiple Patches Using a My Oracle Support Patch Plan" for a list of artifact types that allow multiple patches to be applied in one execution. If one patch fails to apply, the whole process stops.

If any of the patches in the patch plan contains any other artifact types, then Oracle Fusion Applications Patch Manager applies each patch in the plan sequentially, one patch at a time. In this case, the server shutdown and restart occurs multiple times, as required by each patch.

This process of applying multiple patches in a patch plan includes the following steps.

> **Note:** As part of the patching process, customers have their own backup and recovery management process. Oracle recommends that you always have a current backup before applying a patch.

Step 1 Research Issue that Needs to be Resolved by a Patch

When you have an issue that needs to be resolved by one or more patches for Oracle Fusion Applications, file a service request with Oracle Support Services or research the issue on My Oracle Support:

```
http://support.oracle.com
```

Step 2 Check for Existing Patches

After you find patches that may resolve your issues, you should confirm whether you previously applied them to your system. Select one of these options for finding whether patches were applied:

- Run the Patch Status report to see if specific patches were applied, as described in Section 3.5.4, "Patch Status Report".

- Run the Patches Applied report to see all patches applied for a specific product family, as described in Section 3.5.3, "Patches Applied Report".

Step 3 Obtain and Unzip the Patches

Upon determining that you need new patches, create a patch plan and download the patch plan from My Oracle Support. Unzip the patch ZIP files in your PATCH_TOP directory.

Step 4 Read the README File

Read the README file that accompanies each patch. This file contains important information and instructions that must be followed. If a patch contains preinstallation or postinstallation manual steps, they are described in the patch README file. If there are patches listed under "Other Patches" in the README file, you must download and apply them before you apply the Oracle Fusion Applications patch.

Step 5 Validate the Patch

Run the `fapmgr validate` command to alert you to any potential issues that could result in failure while applying the patches. You should resolve all validation failures during this step, to prevent failures during patch application. This validation step is strongly recommended, especially for patches that deliver artifacts whose deployment is automated by Oracle Fusion Applications Patch Manager, such as SOA composites. Note that if you validate a patch that contains BI Publisher artifacts, the BI OPMN control process, which is similar to a node manager, has to be up for online mode validation to succeed.

When you apply patches, the patch validation runs again by default. For more information, see Section 3.3, "Validating Patches".

An example of the `validate` command follows:

```
(UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh validate -grouptop path_to_unzipped_
patches
-patchingplan path_to_patch_plan_xml_file -online
(Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd validate -grouptop path_to_
unzipped_patches
-patchingplan path_to_patch_plan_xml_file -online
```

The patch plan XML is downloaded from My Oracle Support when you download the patch plan.

Step 6 Prepare the System

To prevent locks on patched objects and other data issues during patching of database artifacts, review and perform the following checklist before patching the target environment:

1. Confirm that the database is in an idle state.

2. Confirm that there are no active jobs or processes running against the database. If there are, stop all background jobs, including jobs in the database and active processes

3. Confirm that the Managed Servers are not in "Edit and Lock" mode, so that Oracle Fusion Applications Patch Manager can stop and start servers as needed.

4. Manually shut down the Oracle Enterprise Scheduler Service (ESS) servers, especially when a patch contains a PL/SQL package, by performing the following steps:

   a. Stop the ESS request processor and dispatcher to prevent new requests from being processed. See "Starting and Stopping a Request Processor or Dispatcher" in the *Oracle Fusion Applications Administrator's Guide* for more information.

   b. Cancel any in-progress requests. See "Cancelling Oracle Enterprise Scheduling Server Job Requests" in the *Oracle Fusion Applications Administrator's Guide* for more information.

   c. Shutdown the ESS WebLogic Server Managed server. See the "Starting and Stopping" table, specifically the "Managed Server for an application" row, in the *Oracle Fusion Applications Administrator's Guide* for more information.

5. If any of the patches contain BI Publisher reports, ensure that you have your own versions of any customized BI Publisher reports. If a patch includes an update to a catalog object that was delivered with an Oracle Fusion application, the patch will overwrite any customizations applied to the original report. For more information,

see "Before You Begin Customizing Reports" in the Oracle Fusion Applications Extensibility Guide.

6. If the patch contains BI Publisher artifacts, the BI OPMN control process, which is similar to a node manager, has to be up for online mode validation to succeed.

7. This step is for the Windows operating system only. Ensure that there are no active files. If the lock is not released `fapmgr` will not be able to copy files.

Step 7 Apply the Patches

Apply the patch using the `fapmgr apply` command as described in Section 3.4, "Applying Patches". An example of the `apply` command follows:

```
(UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh apply -grouptop path_to_unzipped_
patches \
-patchingplan path_to_patch_plan_xml_file -online
[-workers number_of_database_workers]

(Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd apply -grouptop path_to_unzipped_
patches \
-patchingplan path_to_patch_plan_xml_file -online [
-workers number_of_database_workers]
```

Step 8 Monitor and Verify the Application of the Patch

Monitor the progress of the patching session and verify its successful completion by reviewing the Log Summary from a browser. For more information, see Section 11.2, "Monitoring Patching Sessions".

Step 9 Verify the Deployment of Middleware Artifacts

Review the Diagnostics report to determine if any artifacts require manual deployment or Managed Servers require restart. For example, this report displays the full path of SOA composites that restarted successfully and those that did not restart successfully, which requires additional manual steps. If any servers must be restarted manually, the report provides the target domain and the names of the cluster and Managed Servers that must be restarted. For more information, see Section 3.5.5, "Diagnostics Report".

You can manually perform these steps or you can use the fapmgr retry command. For more information, see Section 11.3.4, "Retrying Failed Post-Patching Tasks in a Previous Session".

For additional information about the deployment of middleware artifacts, see Section 4.1, "Oracle Fusion Applications Patch Manager Middleware Artifact Support".

4

Patching Oracle Fusion Applications Artifacts

This chapter describes how Oracle Fusion Applications Patch Manager supports middleware and database artifacts. It also provides detailed steps for the manual deployment of artifacts. For more information about applying patches, see Section 3.6, "End-to-End Process for Applying Individual Patches"or Section 3.7, "End-to-End Process for Applying Multiple Patches".

This chapter contains the following topics:

- Oracle Fusion Applications Patch Manager Middleware Artifact Support
- Oracle Fusion Applications Patch Manager Database Artifact Support
- Patching Oracle B2B Metadata
- Patching Oracle Business Intelligence Publisher Artifacts
- Patching Oracle Business Process Management (Oracle BPM) Templates
- Patching C Artifacts
- Patching Common Resource (Activity Strings) Artifacts
- Patching Diagnostic Testing Framework (DTF) JAR Files
- Patching E-Mail and Web Marketing (EWM) Artifacts
- Patching Flexfield Artifacts
- Patching Group Space Templates
- Patching Imaging and Process Management (IPM) Artifacts
- Patching Java EE Artifacts
- Patching Oracle Data Integrator (ODI) Artifacts
- Patching Oracle Fusion Applications Patch Manager Artifacts
- Patching Oracle Fusion Applications Help Content
- Patching Security Artifacts
  - Patching Applications Policies (system-jazn-data.xml)
  - Patching Data Security Grants
  - Patching Data Role (RGX) Templates
  - Patching Data Security Grants and Data Role (RGX) Templates
- Patching Service-Oriented Architecture (SOA) Composites

- [Patching SOAEXTENSION Artifacts](#)
- [Patching SOA Resource Bundles](#)
- [Patching Sales Prediction Engine (SPE) Inline Service Artifacts](#)
- [Patching Tree Artifacts](#)

4.1 Oracle Fusion Applications Patch Manager Middleware Artifact Support

The online mode of Oracle Fusion Applications Patch Manager supports most of the deployment actions required for patching middleware and database artifacts used by Oracle Fusion Applications. Depending on the type of artifact included in a patch, the artifact deployment may require manual actions. Some manual actions are required only if you apply the patch in offline mode, while others are always required. Before applying any patch, Oracle recommends that you run the Patch Impact report to determine which artifact types are included in the patch and actions required by the patch. For more information, see Section 3.5.1, "Patch Impact Report".

Table 4–1 provides a quick reference that depicts how Oracle Fusion Applications Patch Manager supports the Oracle Fusion Middleware artifacts that could be included in a patch. This table assumes that online patching is used unless otherwise specified.

An explanation of the information presented in this table follows:

- Automated Actions Performed by Oracle Fusion Applications Patch Manager

  Oracle Fusion Applications Patch Manager always copies the artifacts from the patch to the appropriate location on your system. This column describes additional actions that are performed automatically in online mode for each artifact.

- Actions to Be Performed Manually in Online Mode

  This column describes the actions you must perform when the patch includes the specified artifact. These actions are described in more detail in this chapter.

- Actions to Be Performed Manually in Offline Mode and in the Case of Failures

  This column describes the actions you must perform when the patch includes the specified artifact and you apply the patch in offline mode. If you apply the patch in online mode and there is a failure, these actions may also be required.

- What Must Be Running During Online Patching Mode and Manual Actions

  This column describes what must be running while applying the patch in online mode and when you perform manual actions.

After you apply a patch, review the Diagnostics report to find out which manual steps are required for the artifacts included in the patch and where the artifacts were copied in *FA_ORACLE_HOME*. For more information, see Section 3.5.5, "Diagnostics Report". For more detailed information about manual actions for each artifact, refer to the relevant sections in this chapter.

Table 4–1   Oracle Fusion Middleware Artifacts Supported by Oracle Fusion Applications Patch Manager

Artifact Type	Automated Actions Performed by Oracle Fusion Applications Patch Manager	Actions to Be Performed Manually in Online Mode	Actions to Be Performed Manually in Offline Mode and in the Case of Failures	What Must Be Running During Online Patching Mode and Manual Actions
Applications Policies (system-jazn-data.xml)	Deploy using the `patchPolicyStore` silent install command for JAZN	Back up the policy store before you apply the patch	Deploy using Oracle Authorization Policy Manager	Oracle Authorization Policy Manager, OPSS Security Store
B2B Metadata	Deploy trading partner agreements	None	Deploy agreements if you want to implement the change	Database
Oracle Business Intelligence Publisher (Reports and Captions)	Shut down the BI Presentation server, deploy to the Business Intelligence repository using Catalog Manager, and start the BI Presentation server after patching	None	Shut down the BI Presentation server, deploy to the Business Intelligence repository using Catalog Manager, and start the BI Presentation server after patching	None
Oracle Business Process Management (Oracle BPM) Template	Publish template to the Oracle Metadata Service (MDS) repository	None	Publish template to the MDS repository	Database
C Artifact	None	None	None	Database must be running. Oracle Enterprise Scheduler Service server must be down.
Common Resource (Activity Strings)	None	Stop and start all Managed Servers in all domains after patching	Stop and start all Managed Servers in all domains after patching	Administration Server, Node Manager, database
Data Security	Run the `DSDataMigrator` utility to reconcile GUID in LDAP	None	Run the `DSDataMigrator` utility to reconcile GUID in LDAP	OPSS Security Store, database
Diagnostic Testing Framework JAR	None	None	None	None
E-Mail and Web Marketing (EWM)	Start and stop the relevant servers that host the Java EE application	None	Start and stop the relevant servers that host the Java EE application	Administration Server, Node Manager, database

Table 4–1   (Cont.) Oracle Fusion Middleware Artifacts Supported by Oracle Fusion Applications Patch Manager

Artifact Type	Automated Actions Performed by Oracle Fusion Applications Patch Manager	Actions to Be Performed Manually in Online Mode	Actions to Be Performed Manually in Offline Mode and in the Case of Failures	What Must Be Running During Online Patching Mode and Manual Actions
Flexfield	Stop and start the FNDSETUP Managed Servers and then deploy the flexfield	None	Stop and start the FNDSETUP Managed Servers and then deploy the flexfield	Administration Server, Managed Servers hosting `FndSetup` application, database
Group Space Template	Deploy template	None	Deploy template	WebCenter Managed Servers (`WC_Spaces`, `WC_Collaboration`), `ucm_server1`, OPSS Security Store, database
Image Routing (IPM)	Deploy to IPM servers	None	Deploy to IPM servers	See prerequisites in Section 4.12.1, "Prerequisites for the Deployment of IPM Artifacts"
Java EE	Stop and start the relevant servers that host the Java EE application	None	Stop and start the relevant servers that host the Java EE application	Administration Server, Node Manager, database
Oracle Data Integrator (ODI)	Import to ODI repository	Drop work tables from FUSION_ODI_STAGE schema after patching	Import to ODI repository and drop work tables from FUSION_ODI_STAGE schema	ODI repository import tool, database
Oracle Fusion Applications Patch Manager	None	Apply the patch with OPatch	Apply the patch with OPatch	None
Oracle Fusion Applications Help Content	None	Stop and restart help portal Managed Servers and start the crawl after patching	Stop and restart help portal Managed Servers and start the crawl after patching	None
Data Role Template (RGX)	Deploy the template	None	Deploy the template	Administration Server, Oracle Authorization Policy Manager, database
SOA Composite	Deploy and merge	Preserve any JDeveloper customizations	Deploy and merge	Administration Server, SOA-INFRA Managed Servers, database
SOAEXTENSION	None	Stop and restart all SOA-INFRA Managed Servers in all domains	Stop and restart all SOA-INFRA Managed Servers in all domains	None

Table 4–1   (Cont.) Oracle Fusion Middleware Artifacts Supported by Oracle Fusion Applications Patch Manager

Artifact Type	Automated Actions Performed by Oracle Fusion Applications Patch Manager	Actions to Be Performed Manually in Online Mode	Actions to Be Performed Manually in Offline Mode and in the Case of Failures	What Must Be Running During Online Patching Mode and Manual Actions
SOA Resource Bundle	Deploy resource bundle and restart dependent composites	Reset SOA-INFRA `MBean` property if resource bundle contains human task-mapped attribute labels and standard view names	Deploy resource bundle and restart dependent composites	Administration Server, SOA-INFRA Managed Servers, Node Manager, database
SPE Inline Service	Deploy SPE files	None	Deploy SPE files	Oracle BI Server, database

4.2 Oracle Fusion Applications Patch Manager Database Artifact Support

Table 4–2 provides a quick reference that displays the Oracle Fusion Applications database artifacts that could be included in a patch. Database artifacts typically do not require manual actions be performed during either online or offline mode. Database artifacts are copied and deployed automatically in both modes. Before patching database artifacts, the database must be in an idle state with no locks being held on any of the database objects. All background jobs, including jobs in the database, must be terminated prior to patching to avoid locks on patched objects. There should not be any active processes, such as Oracle Enterprise Scheduler Service jobs running against the database. This is to prevent locking and other data issues during patching.

Table 4–2   Oracle Fusion Applications Database Artifacts Supported by Oracle Fusion Applications Patch Manager

Artifact Type	Description	Actions to be Performed Manually
Applications Seed Data (XML,XLIFF files)	Examples include static lists of values, functional or error messages, and lookup values. Any non-transactional data values loaded into your database can be considered seed data.	Oracle recommends that patches containing seed data be applied from a machine that is co-located in the same subnetwork as the database server to maximize performance.
Applications Database schema changes (SXML)	Examples include tables, triggers, views, sequences, synonyms, queues, queue tables, policies, and contexts.	None
PL/SQL objects (pkh, pkb files)	Package headers and bodies.	Manually shut down the Oracle Enterprise Scheduler Service servers before applying patches that contain PL/SQL changes.
SQL scripts	Scripts that update the database.	None

4.3 Patching Oracle B2B Metadata

Oracle recommends that you patch Oracle B2B metadata in online mode. When updates to Oracle B2B metadata are introduced in a patch, no manual steps are required in online mode to redeploy all Trading Partner Agreements that are affected by the metadata change.

4.3.1 Manually Deploying Trading Partner Agreements

If you choose to apply a patch containing Oracle B2B metadata updates in offline mode, and you want to implement the change, you must manually redeploy all Trading Partner Agreements that are affected by the metadata change. If you do not perform the redeployment, the runtime continues to use the older metadata. You can deploy the agreements using the B2B User Interface (UI) or by running the `b2bdeploy` utility from the command line.

4.3.1.1 Deploying Agreements from the User Interface

To deploy all agreements from the UI, follow the steps in "Deploying an Agreement" in the *Oracle Fusion User's Guide for Oracle B2B*.

4.3.1.2 Deploying Agreements from the Command Line

To import the patched metadata and deploy the agreements, follow these steps:

1. Follow the steps in "Prerequisites for Running the Command-line Tools" in the *Oracle Fusion User's Guide for Oracle B2B* with one exception. In Step 2 under "Create jndi.properties", you must use this command:

   ```
   cd FA_ORACLE_HOME\soa\bin
   ```

   instead of this command:

   ```
   cd $ORACLE_HOME\bin
   ```

2. Export the entire repository for backup purposes.

   ```
   ant -f ant-b2b-util.xml b2bexport -Dexportfile=/tmp/backup_export.zip
   ```

3. Import the patched export file.

   ```
   ant -f ant-b2b-util.xml b2bimport -Dexportfile=/tmp/patch_export.zip
   -Dlocalfile=true -Doverwrite=true
   ```

4. Run the `b2bdeploy` command. If there is no Trading Partner Agreement found, this step is not needed.

   ```
   ant -f ant-b2b-util.xml b2bdeploy -
   Dtpanames="Agreement_name,Agreement_name"
   ```

5. If the patch introduces new documents for Trading Partner agreements, you must add the document definition. For more information, see "Adding Document Definitions" in the *Oracle Fusion Middleware User's Guide for Oracle B2B*.

For more information about the `b2bdeploy` command, see "Deploying Agreements" in the *Oracle Fusion User's Guide for Oracle B2B*.

4.4 Patching Oracle Business Intelligence Publisher Artifacts

When you patch Oracle Business Intelligence Publisher (BI Publisher) artifacts (Reports and Captions) in online mode, Oracle Fusion Applications Patch Manager

shuts down the BI Presentation Server before the patch applies and restarts it after successful patch application. No manual steps are required in online patching mode. If the shutdown of this server fails for any reason, you must manually deploy the BI Publisher artifacts.

Oracle recommends you do not use offline mode when a patch contains BI Publisher artifacts. If you decide to apply a patch in offline mode, you must manually deploy the changes to the Oracle Business Intelligence repository in addition to stopping and restarting the BI Presentation server. These manual steps are required to keep the Oracle home and the Oracle Instance versions of the Oracle Business Intelligence Presentation Catalog synchronized. If these manual steps are not followed as described, subsequent patches containing BI Publisher artifacts may fail.

For more information, see "Starting and Stopping Oracle Business Intelligence" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*.

4.4.1 Prerequisites for Manual BI Publisher Artifact Deployment

The following must occur before manual deployment of BI Publisher artifacts:

1. The `opmn` processes must be running. Follow these steps:

    a. To verify if the process is running, go to the *FA_ORACLE_HOME*`/instance/BIInstance/bin` and run this command:

       ```
       opmnctl status
       ```

    b. If the opmn process is not alive, start it with this command:

       ```
       opmnctl start
       ```

2. Oracle Fusion Applications Patch Manager copies one or more Oracle BI Presentation Catalog files into the Oracle home-based catalog.

3. Within the patch, there are some catalog *diff* files. These files are used with the Oracle Business Intelligence Catalog Manager tool to apply changes to a catalog. These changes must be applied to:

    ■ The run-time, or Oracle Instance, Oracle BI Presentation Catalog

    ■ The Oracle home Oracle BI Presentation Catalog

4. Special care must be taken when the patch being applied is a standard patch. With a standard patch, OPatch may choose to copy only a subset of the total files in the patch archive.

    Before performing the steps in Section 4.4.2, "Manually Deploying BI Publisher Artifacts", you must first determine exactly which files were actually copied to the Oracle home during the OPatch apply stage. You can review the Patch Impact report to get this list of files. You can also capture the list of files from the messages sent to the console and to the `FAPatchManager_apply_`*timestamp*`.log` file.

    After you have that list, you must apply only the *diff* files that correspond to the files that were actually copied to the Oracle home. The *diff* files are named the same as the original files, except they have a *.diff* extension added. If additional *diff* files are applied beyond the files that were actually copied to the Oracle home, then previous patch updates may be undone and the Oracle BI Presentation Catalog may be in an unsupportable state. Basically, you have partially rolled back a previous patch.

4.4.2 Manually Deploying BI Publisher Artifacts

Follow these steps to manually deploy BI Publisher artifacts:

1. Shut down the BI Presentation server.

2. Unzip the middleware portion of the patch, the OPatch archive file, into a temporary location, such as `C:\patch`. To see which files are included in the patch, run the Patch Impact report. For more information, see Section 3.5.1, "Patch Impact Report".

3. Using the example in Step 2, go to the `C:\patch\custom\scripts` directory.

4. Locate the Catalog Manager *diff* files listed in the subdirectories under the directory in Step 2. These files have *.diff* extensions.

5. Use Catalog Manager to apply each of these *diff* files to the Oracle home Oracle BI Presentation Catalog, using the following commands:

   a. Create the Catalog Manager patch file.

   ```
   oracle-instance/runcat.cmd -cmd createPatch -inputFile diff_file_location
    -production webcat_location -outputFile webcat_patch.out -winsConflict
   latest
   ```

   – *diff_file_location* refers to the file from Step 4.

   – *webcat_location* is the Oracle home Oracle BI Presentation Catalog location.

   – *webcat_patch.out* is a temporary file created by this step and used in Step 5b.

   Example of `oracle-instance` on Unix:

   ```
   APPLICATIONS_BASE/instance/BIInstance/bifoundation
   /OracleBIPresentationServicesComponent/coreapplication_
   obips1/catalogmanager
   ```

   Example of `oracle-instance` on Windows:

   ```
   C:\APPLICATIONS_BASE\instance\BIInstance\bifoundation
   \OracleBIPresentationServicesComponent\coreapplication_
   obips1\catalogmanager
   ```

   b. Apply the Catalog Manager patch file.

   ```
   oracle-instance/runcat.cmd -cmd applyPatch -inputFile webcat_patch.out
   -outputFile  -persistNewApplicationsRoles webcat_applypatch.out
   ```

   – *webcat_patch.out* is the file created in Step 5a.

   – *webcat_applypatch.out* is the output file from this deployment process.

6. Repeat Step 5 for the run-time catalog.

7. Restart the Oracle Business Intelligence system components using `opmnctl`:

   ```
   cd APPLICATIONS_BASE/instance/BIInstance/bin/opmnctl
   ./opmnctl stopall
   ./opmnctl startall
   ```

4.5 Patching Oracle Business Process Management (Oracle BPM) Templates

Oracle recommends that you patch Oracle BPM templates in online mode. When updates to Oracle BPM templates are introduced in a patch, no manual steps are required in online mode to publish the new Oracle BPM Template to the Oracle Metadata Service (MDS) repository.

4.5.1 Manually Publishing Oracle BPM Templates

If you choose to apply a patch containing updates to Oracle BPM templates in offline mode, you must manually publish the new Oracle BPM Template to the Oracle Metadata Service (MDS) repository supporting the Oracle BPM Composer instance after you apply the patch. You use the `publish_template` WebLogic Scripting Tool (WLST) command from the WLST shell. The WLST `publish_template` command connects to the SOA MDS data using the `mds-config.xml` configuration file that you create. You must provide the location of the `mds-config.xml` configuration file as one of the input parameters of the `publish_template` command.

4.5.1.1 Creating the mds-config.xml Configuration File

Follow these steps to create the mds-config.xml configuration file:

1. Copy the `mds-config-template.xml` file from your SOA server installation to a temporary directory.

   ```
   cp SOA_ORACLE_HOME/bpm/config/mds-config-template.xml /tmp/mds-config.xml
   ```

2. Modify the following properties in the file you just copied to the temporary directory:

   - Set `jdbc.userid` to the database user name of the SOA MDS database

   - Set `jdbc.passwd` to the database password of the SOA MDS database

   - Set `jdbc.url` to the connection URL of the SOA MDS database, for example, `jdbc:oracle:thin:@host2:1525:mds`

   - Set `partition.name` to `obpm`

4.5.1.2 Publishing the New Oracle BPM Template to the MDS Repository

Follow these steps to publish the new Oracle BPM template to the MDS repository:

1. Review the Diagnostics report to find the location of the archive file that contains the BPM template. For more information, see Section 3.5.5, "Diagnostics Report".

2. Expand the archive that contains the new BPM template, so the `publish_template` command can find the template.

   - Create or use an existing temporary directory.

   - Untar the patched archive file, as shown in this example:

     ```
     cd /tmp
     mkdir preboardWorker
     cd preboardWorker
     jar xf FA_ORACLE_HOME/hcm/deploy/bta_
     HcmCommonProcessesPreboardWorkerComposite.jar
     ```

3. Access the WLST shell.

   ```
   (UNIX) SOA_ORACLE_HOME/common/bin/wlst.sh
   ```

```
(Windows) SOA_ORACLE_HOME\common\bin\wlst.cmd
```

4. Deploy the Oracle BPM template, passing the temporary directory, /tmp/preboardWorker, as the directory containing the template in the example in Step 2.

Generic command syntax follows:

```
publish_template(templateName, fsLocation, mdsconfigLocation, [Override],
[oracleHome] )
```

See "publish_template" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference* for more information about the publish_template command syntax.

Note that the publish_template command simply updates the existing Oracle BPM template with a newer version. It has no impact on the projects deployed or instantiated from the existing template.

4.6 Patching C Artifacts

When updates to C artifacts are introduced in a patch, no manual steps are required in either online or offline mode. Note that before applying C artifacts, all C executable files and the Oracle Enterprise Scheduler Service servers that host the C files must be shut down and the database must be running. For more information, see "Starting and Stopping Oracle Enterprise Scheduler Service Components" in the *Oracle Fusion Applications Administrator's Guide*.

4.7 Patching Common Resource (Activity Strings) Artifacts

When updates to Common Resource artifacts are introduced in a patch, the Administration Server, Node Manager, and database must be running. You must stop and restart all Managed Servers in all domains after you apply the patch.

4.8 Patching Diagnostic Testing Framework (DTF) JAR Files

No manual steps are required when patching DTF artifacts in either online or offline mode.

4.9 Patching E-Mail and Web Marketing (EWM) Artifacts

Oracle recommends you patch EWM artifacts in online mode. When updates to EWM artifacts are introduced in a patch, no manual steps are required in online mode. In offline mode, follow the steps in Section 4.13, "Patching Java EE Artifacts".

4.10 Patching Flexfield Artifacts

Oracle recommends that you patch flexfield artifacts in online mode. When flexfield changes are introduced in a patch, no manual steps are required to automatically deploy the flexfields in online mode, except to ensure that the following are running:

- Administration Server
- Managed Servers that host the FndSetup application
- Database

Users must log out and log in after a successful patch application to see the latest flexfield changes because flexfields reload upon user logout and login. If you decide that you do not want to implement the changes to a flexfield, you can revert to a previous version of a flexfield. For more information, see Section 11.3.9, "Revert To a Previous Flexfield Definition After It Is Updated By a Patch".

4.10.1 Manually Deploying Patched Flexfields

Follow these steps after patching flexfields in offline mode to manually deploy the patched flexfields.

1. Ensure that the Administration Server and database are running.

2. Stop and start the FNDSETUP Managed Servers. For more information, see "Starting and Stopping" in the *Oracle Fusion Applications Administrator's Guide*.

3. Connect to the Oracle WebLogic Server Administration Server for the domain that hosts the FndSetup application. This is typically the Common Domain.

4. Run the deployPatchedFlex() WLST command. Because you run this on a domain that hosts the FndSetup Application, you do not have to specify this application within the parentheses. However, the FndSetup application must be running for the command to succeed.

    Example:

    ```
    connect('weblogic' , 'weblogic1' , 't3://localhost:7101')
    deployPatchedFlex()
    ```

5. Review the report for errors.

Example of confirmation that flexfield changes were successfully deployed

As an example, assume that the patch delivered a new flexfield segment to the Calculation Defaults in Payroll Definitions. To confirm that the new flexfield segment was successfully deployed, follow these steps in your Payroll application:

1. From your Oracle Fusion Payroll application, select **Manage Payroll Definition**.

2. Click the **Create a New Payroll** icon.

3. Select a **Legislative Data Group**.

4. Confirm that the new flexfield segment appears under **Calculation Defaults**.

4.11 Patching Group Space Templates

When a Group Space template is included in a patch, the patch introduces a new template with a version number attached, which is unlike other artifacts where the patched version replaces the existing one. If you have any customizations on this template that the patched version will replace, you must manually incorporate the customizations in the new version of the template. If you have any settings or configurations that refer to the Group Space template name, ensure that you update these to reflect the new template name. For all WebCenter services configured in a Group Space template, ensure that connections are configured properly.

Oracle recommends that you patch Group Space templates in online mode. When updates to Group Space templates are introduced in a patch and you have not customized the template included in the patch, no manual steps are required in online mode, except to ensure that the following servers must be running:

■   WebCenter Managed and Servers: WC_Spaces, WC_Utilities

- Oracle UCM Managed Server, `ucm_server1`
- LDAP Policy Store Server

4.11.1 Manually Deploying Group Space Templates

In offline mode, or in the case of failure, you must manually deploy the new Group Space template using the `importGroupSpace` WLST command.

1. Ensure that the following WebCenter Managed Servers are running:
   - WebCenter Managed Servers: `WC_Spaces`, `WC_Utilities`
   - Oracle UCM Managed Server, `ucm_server1`
   - LDAP Policy Store Server

2. Access the WLST shell from the Oracle home where WebCenter is installed.

   ```
   (UNIX) WC_ORACLE_HOME/common/bin/wlst.sh
   (Windows) WC_ORACLE_HOME\common\bin\wlst.cmd
   ```

3. Deploy the Group Space template.

   ```
   importGroupSpaces('appName', 'fileName')
   ```

   The `appName` is always `webcenter` and the `fileName` is the name of the WebCenter archive file, from the patch, that you want to import. Refer to the Diagnostics report to get the full path and file name. For more information, see Section 3.5.5, "Diagnostics Report".

   For more information, see "importGroupSpaces" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*. For more information about Group Space templates, see "Importing Space Templates" in the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter*.

4.12 Patching Imaging and Process Management (IPM) Artifacts

Oracle recommends you patch IPM artifacts in online mode. When updates to IPM artifacts are introduced in a patch, no manual steps are required in online mode, other than ensuring all prerequisites are met. In offline mode, you must manually deploy the IPM artifacts.

4.12.1 Prerequisites for the Deployment of IPM Artifacts

1. The opmn processes must be running. Follow these steps:

   a. To verify if the process is running, go to the *FA_ORACLE_ HOME*/`CommonDomain_webtier` directory and run this command:

   ```
   opmnctl status
   ```

   b. If the opmn process is not **Alive**, start it with this command:

   ```
   opmnctl start
   ```

2. The imaging application must be running. The format for the IPM URL is `http://<host name>:<Port>/imaging/`.

3. The Financials SOA server (`soa_server1`) must be running.

4. The Financials Payables Invoice and Expense Report SOA composites must have been successfully deployed and be in an active state.

5. The `FIN wsm-pm` application must be in an active state, which means your `FinancialCommon` server must be running.

6. The IPM to UCM connection, "Fusion Applications UCM Connection", must exist.

7. The IPM to SOA connection, "Financial SOA Connection", must exist.

8. The IPM Input should be set to **Offline** from the **Manage Inputs** section of the IPM UI. For example, select **Invoices** under **Manage Inputs** and then deselect **Online** under **Basic Information**.

9. Follow these steps to back up the existing IPM application definition:

    a. Log in to the IPM server as the IPM superuser.

    b. From **Tools**, select **Export Definitions**.

    c. Export your Oracle Fusion Payables Application and Expenses Application, all related searches, and inputs to a local file.

4.12.2 Manually Deploying IPM Artifacts

1. Review the Diagnostics report to find the location of the IPM artifacts that were copied to *FA_ORACLE_HOME*. For more information, see Section 3.5.5, "Diagnostics Report".

2. Access the WLST shell.

    ```
    (UNIX) ECM_ORACLE_HOME/common/bin/wlst.sh
    (Windows) ECM_ORACLE_HOME\common\bin\wlst.cmd
    ```

3. Deploy the IPM artifact.

    ```
    connect(IPM Server user name,IPM Server password,IPM Server hostname:port)
    importIPMApplication(ipmAppFile,'Update',appDefName,'None');
    importIPMInput(ipmAppFile,'Update',inputDefName);
    ```

    Example:

    ```
    connect('FAadmin','fusion','t3://server01.us.oracle.com:17014');

    importIPMApplication(exportFile='/net/server01/fusionapps/applications/fin/ap/i
    pm/ApInvoiceIpmApp.xml', action='Update', name='Payables Invoice
    Application','None')

    importIPMInput(exportFile='/net/server01/fusionapps/applications/fin/ap/ipm/ApI
    nvoiceIpmApp.xml', action='Update', name='Payables Invoice Input')
    ```

4. If applicable, perform your customizations on the new file, based on the file you exported.

4.13 Patching Java EE Artifacts

Oracle recommends that you patch Java EE artifacts in online mode. When you patch Java EE artifacts in online mode, no manual steps are required, except to ensure that the following are running:

-   Administration Server
-   Node manager
-   Database

In offline mode, you must manually stop, patch, and restart the impacted Managed Servers that host the Java EE application. To determine which product family is affected by the patch you are applying, run the Patch Impact report. For more information, see Section 3.5.1.1, "Running the Patch Impact Report". For example, if the Patch Impact report indicates that the patch updates a Java EE artifact in the Financials Domain, then you stop the Financials Domain, apply the patch, and then start the Financials Domain after the patch applies successfully. Examples of artifacts in this category include Oracle ADF Resource JAR files and Oracle Enterprise Scheduler Service MAR files.

For more information about stopping and starting servers, see "Starting and Stopping a Product Family Oracle WebLogic Server Domain" in the *Oracle Fusion Applications Administrator's Guide*.

4.14 Patching Oracle Data Integrator (ODI) Artifacts

Oracle recommends that you patch ODI artifacts in online mode. When updates to ODI artifacts are introduced in a patch, Oracle Fusion Applications Patch Manager imports the ODI changes in online mode. If you patch ODI artifacts in offline mode, you must manually import the changed ODI content to the ODI repository. In both online and offline modes, the ODI repository import tool and the database must be running and you must manually drop the work tables from the FUSION_ODI_STAGE schema.

> **Note:** Oracle Fusion Applications Provisioning does not install ODI Studio. You must install ODI Studio before manually importing ODI changes, for example, after you apply patches that deliver ODI changes in offline mode or when you need to manually retry a failed ODI import step in online mode. For more information, see "Installing Oracle Data Integrator" in the *Oracle Fusion Middleware Installation Guide for Oracle Data Integrator*.

4.14.1 Dropping Work Tables After Patching in Online Mode

After you apply a patch that contains ODI artifacts in online mode, you must manually drop the work tables from the schema, FUSION_ODI_STAGE.

1. Connect to the Oracle Fusion Applications database with the correct privilege.

2. Drop all tables that begin with **E$** from the FUSION_ODI_STAGE schema.

4.14.2 Manually Importing ODI Changes

Oracle recommends that the ODI import be performed from a machine that is co-located in the same subnetwork as the database server to maximize performance.

1. Review the instructions in the patch README file to determine which ODI Project or Model must be deleted and imported again. The patch README file contains a list of the ODI files that are included in the patch, in the order that they must be imported.

2. Review the Diagnostics report to determine the location and file name for each ODI artifact that is to be imported. For more information, see Section 3.5.5, "Diagnostics Report".

3. Start the ODI Studio.

   ```
   (UNIX) odi.sh
   ```

```
(Windows) odi.exe
```

4. Access the ODI Studio.

    a. Select **View**, then **ODI Designer Navigator**.

    b. Click **Connect to Repository**.

    c. Log in using the superuser name and password for the ODI repository.

    For more information, see "Connecting to a Work Repository" in the *Oracle Fusion Middleware Developer's Guide for Oracle Data Integrator*.

5. Delete the Model or Project if specified in the patch README file. The README file specifies whether any Model or Project must be deleted and in what order.

    Right-click the Model or Project name and click **Delete**.

6. Import the ODI files in the order they are listed in the patch README file.

    a. To import a project, right-click the Project name and click **Import**, then **Import Project.**

    b. To import a model, right-click the Model name and click **Import**, then **Import Model**.

    c. Select **Synonym Mode INSERT_UPDATE** from the list in the Import Dialog window.

    d. For the File Import directory, select the directory that contains the ODI file you want to import.

    e. Select the ODI file to import.

    f. Click **OK** to import.

    Repeat Steps 5 and 6 for each Model or Project in the patch.

    For more information, see "Exporting/Importing" in the *Oracle Fusion Middleware Developer's Guide for Oracle Data Integrator*.

7. Close the ODI Studio after importing all the files in the order specified in the patch README file.

8. Connect to the Oracle Fusion Applications database with the correct privilege.

9. Drop all tables that begin with **E$** from the FUSION_ODI_STAGE user.

4.15 Patching Oracle Fusion Applications Patch Manager Artifacts

When updates to Oracle Fusion Applications Patch Manager are introduced in a patch, you must apply the patch with the OPatch utility. For more information, see "Patching Oracle Fusion Middleware with Oracle OPatch" in the *Oracle Fusion Middleware Patching Guide*.

During provisioning, the data model for Oracle Fusion Applications Patch Manager is updated by running the fapmgr bootstrap command. If the data model is updated again by a patch, the patch README file instructs you to run the fapmgr bootstrap command.

Use this syntax to run bootstrap:

```
(UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh bootstrap [-logfile log_file_name]
[-loglevel level]

(Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd bootstrap [-logfile log_file_name]
```

```
[-loglevel level]
```

4.16 Patching Oracle Fusion Applications Help Content

Oracle Fusion Applications Help requires content patches to ensure that users do not encounter a "Help Unavailable" message and to make certain the version of help is available to users for subsequent releases. There can be multiple patches required for the delivery of the latest version of Oracle Fusion Applications Help. If more than one patch is required for an update, the required patches are listed as prerequisite patches. You must apply all required patches to avoid broken links. Refer to the Oracle Fusion Applications release notes to get the patch numbers for the latest version of Oracle Fusion Applications Help.

Standard patches of help content may be published from time to time. These patches contain two types of content:

- A Seed Data Files patch that containing updated help topics that you apply using Oracle Fusion Applications Patch Manager.

- Reference content patches that may contain:

  - BPM diagrams

  - User Productivity Kit demos

  - Oracle Fusion Applications Technology library

To apply Oracle Fusion Applications Help patches

1. Run the Patch Impact report to determine the patch content. For more information, see Section 3.5.1, "Patch Impact Report".

2. To apply Oracle Fusion Applications Help reference patches, unzip the patch file and move the content to the equivalent directory in your *APPLICATIONS_BASE*, where *APPLICATIONS_BASE* is the root directory under which the provisioned environment resides. Apply the patches with Oracle Fusion Applications Patch Manager. For more information about applying Oracle Fusion Applications patches, see Section 3.4, "Applying Patches".

3. Stop and restart the help portal Managed Servers in the `HelpPortalCluster` in the Common Domain after the patch is successfully applied.

4. Manually start the crawl using Oracle Enterprise Crawl and Search Framework (ECSF) so users can see the results immediately. You can create or modify an index schedule to run manually and then start the schedule. If you do not manually start the index schedule, the content will be included during your next scheduled index schedule. For more information about ECSF scheduling, see "Managing Index Schedules" in the *Oracle Fusion Applications Administrator's Guide*.

4.17 Patching Security Artifacts

In Oracle Fusion Applications, the following artifact types related to security can be patched:

- Function Security Policies (Applications Policies, using the `system-jazn-data.xml` file)

- Data Security Grants (using Seed Data)

- Data Role (RGX) Templates

■ JAR files secured by the Data Security Grants and Function Security Grants

A patch can contain one or more of these artifacts. This section describes the steps for applying security patches and recovering from patch failures. Examples of scenarios when you may need to follow the recovery steps include:

■ You apply a security patch that introduces a set of new policies and LDAP GUIDs, after backing up the policy store and the applications database. You have not performed the GUID reconciliation with the applications database due to an unrelated database issue. To resolve the database issue, you restore from the backup, resulting in the policy store containing extra GUIDs from the database and a synchronization issue between the policy store and the database.

■ You apply a security patch that includes updates to the applications policies and the patch fails, resulting in a set of LDAP GUIDs not applying correctly.

The patching and recovery scenarios for the following combinations of security artifact patches are included:

■ Patching Applications Policies (system-jazn-data.xml)

■ Patching Data Security Grants

■ Patching Data Role (RGX) Templates

■ Patching Data Security Grants and Data Role (RGX) Templates

■ Backing up the Data Security Store

■ Recovering Data Security Seed Data from the Backup

Oracle recommends that you apply security patches in online mode and run the Patch Impact report to understand which artifacts are included in the patch. The Patch Impact report displays security artifacts as JAZN, Data Security, and RGXTEMPLATE. For more information, see Section 3.5.1, "Patch Impact Report".

For more information about general troubleshooting for Oracle Fusion Applications Patch Manager, see Chapter 11, "Monitoring and Troubleshooting Patches". For more information about security in Oracle Fusion Applications, see "Securing Oracle Fusion Applications" in the *Oracle Fusion Applications Administrator's Guide*.

4.17.1 Patching Applications Policies (system-jazn-data.xml)

Oracle Fusion Applications uses the XML file system-jazn-data.xml to package function security policies through application roles, role hierarchies, grants, and policies. Function security policies are shipped as a system-jazn-data.xml file that resides in the Oracle home. After provisioning, these policies are migrated to an LDAP Policy store. Patching function security policies requires steps to absorb changes delivered by Oracle (system-jazn-data.xml in a patch), changes currently deployed, which include changes by you (policies in the LDAP server), and system-jazn-data.xml contents previously shipped from Oracle (system-jazn-data.xml in the Oracle home).

Oracle Fusion Applications Manager runs a comprehensive analysis tool during patch validation to check for conflicts in applications policy changes before you apply the patch. If a change is considered *safe*, you can apply the patch in online mode. If a change is considered to be a *conflict*, you must follow the steps to apply the patch in offline mode, which includes manually resolving conflicts. Table 4–3 describes a summary of changes that are safe and those that cause a conflict.

Table 4–3   Changes to Applications Policies

Type of Change	Safe - Apply Patch in Online Mode	Conflicts - Apply Patch in Offline Mode
Additions	New artifacts shipped from Oracle.	Artifacts retained by Oracle in a patch with or without modifications, but deleted by the customer.
Modifications	Artifacts modified by Oracle in a patch but not by the customer.	■ Artifacts modified by Oracle in a patch and by the customer. ■ Artifact created by both Oracle in a patch and by the customer, using the same identifier, but with some other differences.
Deletions	All artifact deletions must be applied in offline mode.	■ Artifacts deleted by Oracle in a patch and not touched by the customer. ■ Artifacts deleted by Oracle in a patch and modified by the customer. ■ Artifacts deleted by Oracle in a patch, and where the customer created new references to the Oracle deleted artifact in their system. Examples include but are not limited to permission and resource grants, entitlements grants, role inheritance relationships, and entitlements to resource associations.

For more information about what the `system-jazn-data.xml` file contains, see the "The OPSS Policy Model" chapter in the *Oracle Fusion Middleware Security Guide*. For more information about patching applications policies, see the "Upgrading Oracle Fusion Applications Policies" chapter in the *Oracle Fusion Middleware Oracle Authorization Policy Manager Administrator's Guide (Oracle Fusion Applications Edition)*.

This section contains information about the following methods for patching applications policies:

■ Prerequisites for Patching Applications Policies in Online Mode

■ Patching Applications Policies in Offline Mode With Authorization Policy Manager

4.17.1.1 Prerequisites for Patching Applications Policies in Online Mode

Oracle recommends that you patch applications policies in online mode because Oracle Fusion Applications Patch Manager automates the deployment of the `system-jazn-data.xml` file by running the `patchPolicyStore` silent install command.

Ensure that the following steps are completed before patching applications policies in online mode.

1. Validate the patch in online mode and ensure that the validation output does not contain any conflicts. For more information, see Section 3.3, "Validating Patches" and Table 4–3, " Changes to Applications Policies".

   If the validation reports any conflicts, then you can choose to apply all safe changes in online mode. Later, you must apply conflicting changes in offline mode, as described in Section 4.17.1.2, "Patching Applications Policies in Offline Mode With Authorization Policy Manager".

2. Back up function security policies in the Oracle Internet Directory (OID) Policy store by following the steps in "Prerequisites to Patching Policies" in the *Oracle*

Fusion Middleware Oracle Authorization Policy Manager Administrator's Guide (Oracle Fusion Applications Edition).

3. All domains that use the OPSS Policy store in OID for authorization policies must be shut down before the patch applies.

4.17.1.2 Patching Applications Policies in Offline Mode With Authorization Policy Manager

The following steps must be performed if you patch applications policies in offline mode using Authorization Policy Manager (APM).

> **Note:** All domains, except the OPSS Security Store and the domain that hosts APM, must be shut down before JAZN patching and restarted after JAZN patching.

1. Run the Patch Impact report to see which artifacts are included in the patch. For more information, see Section 3.5.1, "Patch Impact Report". Note the location where `system-jazn-data.xml` is located in the patch, because you are prompted for this location in Step 4.

2. Back up function security policies in the Oracle Internet Directory (OID) Policy store by following the steps in "Prerequisites to Patching Policies" in the *Oracle Fusion Middleware Oracle Authorization Policy Manager Administrator's Guide (Oracle Fusion Applications Edition)*.

3. Run Oracle Fusion Applications Patch Manager to apply the patch, which copies `system-jazn-data.xml` from the patch to the Oracle home in offline mode. For more information, see Section 3.4, "Applying Patches".

4. Log in to Authorization Policy Manager.

5. Open the **Policy Upgrade Management** tab. Follow the steps in "The Policy Upgrade Management Tab" in the *Oracle Fusion Middleware Oracle Authorization Policy Manager Administrator's Guide (Oracle Fusion Applications Edition)*. When you select the application to patch from the pull-down **Application** list, you should see choices such as the following:

   - `fscm_system-jazn-data.xml: FSCM stripe`

   - `crm_system-jazn-data.xml: CRM stripe`

   - `hcm_system-jazn-data.xml: HCM stripe`

   - `bip_jazn-data.xml: OBI stripe`

6. Follow the steps in "Analyzing Patch Differences" and "Resolving Patch Differences" in the *Oracle Fusion Middleware Oracle Authorization Policy Manager Administrator's Guide (Oracle Fusion Applications Edition)*. If there are any errors during this step, restore the backup, as described in "Prerequisites to Patching Policies" in the *Oracle Fusion Middleware Oracle Authorization Policy Manager Administrator's Guide (Oracle Fusion Applications Edition)*.

7. Restart all Oracle Fusion Applications domains.

8. Oracle delivers changes to `system-jazn-data.xml` in its own patch. Related code change patches, if any, should be applied only after all of the steps in this section complete successfully.

4.17.2 Patching Data Security Grants

Oracle recommends that you patch data security grants in online mode. When data security grant changes are introduced in a patch, no manual steps are required in online mode to update the data security subsystem with the GUIDs of new application roles seeded in the policy store. In offline patching mode, you must manually run the `DSDataMigrator` utility as described in "Reconciling GUIDs" in the *Oracle Fusion Applications Administrator's Guide*. In both online and offline patching mode, you must ensure that the prerequisites are met.

4.17.2.1 Prerequisites for Patching Data Security Grants

1. Run the Patch Impact report to see which artifacts are included in the patch. For more information, see Section 3.5.1, "Patch Impact Report".

2. Back up the data security store by using the Oracle Database data pump export tool. For more information, see Section 4.17.5, "Backing up the Data Security Store".

4.17.2.2 Patching Data Security Grants

Follow these steps to patch data security steps:

1. Run Oracle Fusion Applications Patch Manager to apply the seed data changes to the data security system. For more information, see Section 3.4, "Applying Patches". When data security changes are introduced in a patch, no manual steps are required in online mode to update the data security subsystem with the GUIDs of the new application roles seeded in the policy story. In offline mode or in the case of patch failure, you must manually run the `DSDataMigrator` utility as described in "Reconciling GUIDs" in the *Oracle Fusion Applications Administrator's Guide*.

2. If there are any database errors during Step 1, such as running out of tablespace, fix the database errors that occurred and restart the patch.

3. If you are unable to resolve the errors that occurred while applying the seed data changes, recover the seed data from the backup export file you created in Step 2 of the prerequisites. For more information, see Section 4.17.6, "Recovering Data Security Seed Data from the Backup".

4.17.3 Patching Data Role (RGX) Templates

Oracle recommends that you patch data role templates in online mode. When data role template changes are introduced in a patch, no manual steps are required in online mode to deploy the changed templates.

4.17.3.1 Manually Deploying Data Role (RGX) Templates

Follow the steps in this section when you apply a patch in offline mode that contains data role templates. Every data role template consists of two XML files. One is for data role generation and the other XML file is for data security policies generation. Both of these files must be deployed after you apply a patch that contains changes to data role templates, so they remain synchronized with each other.

1. Run the Patch Impact report to see which artifacts are included in the patch. For more information, see Section 3.5.1, "Patch Impact Report". Note that the Patch Impact report refers to data role templates as `RGXTEMPLATE`.

2. The following must be running while patching data role templates:

   - Administration Server

- Oracle Authorization Policy Manager

- Database

3. Run Oracle Fusion Applications Patch Manager to copy the data role templates to *FA_ORACLE_HOME*. For more information, see Section 3.4, "Applying Patches".

4. To create a save point before deploying the data role templates, use the `createMetadataLabel` WLST command to label the MDS partition for `oracle.security.apm`, using the following syntax:

```
createMetadataLabel(application, server, name)
```

The following example creates the label `data_role_save_point` for the application `oracle.security.apm` deployed in the Administration Server:

```
createMetadataLabel('oracle.security.apm', 'AdminServer', data_role_save_
point')
```

For more information, see "createMetadataLabel" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

5. Follow these steps to manually deploy the data role templates using the `importMetadata` WLST command against the Administration Server in the Common Domain for the `oracle.security.apm` application:

   a. Access the WLST shell.

   ```
   (UNIX) SOA_ORACLE_HOME/common/bin/wlst.sh
   (Windows) SOA_ORACLE_HOME\common\bin\wlst.cmd
   ```

   b. Connect to WebLogic Server.

   ```
   > connect ('admin user name','admin user password','URL of the
   AdminServer')
   ```

   c. Deploy the data role template using the `importMetadata` WLST command. Refer to the Diagnostics report to find the directory where the template was copied. For more information, see Section 3.5.5, "Diagnostics Report".

   Syntax for the `importMetadata` command:

   ```
   importMetadata(application='oracle.security.apm', server='Name of
   AdminServer',
   fromLocation='Directory in FA_ORACLE_HOME where data role templates were
   copied',
   docs='Path to the changed data role templates starting with APM partition')
   ```

   Table 4–4 displays the parameters required by the `importMetadata` command.

Table 4–4   Parameters for the importMetadata WLST Command

Parameter Name	Description
application	Enter the value of `oracle.security.apm`

Table 4–4   (Cont.) Parameters for the importMetadata WLST Command

Parameter Name	Description
server	Enter the name of your Administration Server
fromLocation	Enter the absolute path to the directory in *FA_ORACLE_HOME* where the patch copied the data role templates. The path must not include the APM partition, because the APM partition is included in the next parameter, docs. The Diagnostics report provides the full path and file name in *FA_ORACLE_HOME* for each data role template that was copied from the patch.
docs	Enter the directory for the APM partition, starting with /oracle/apps/apm, followed by the remainder of the path, which includes the data role template itself.

Example 4–1   Importing the FinancialAssetBook.xml data role template

In this example, the FinancialAssetBook.xml data role template is located in this directory:

```
(UNIX)FA_ORACLE_HOME/fin/fa/apm/oracle/apps/apm/fin/fa/rgx/template
```

```
(Windows)FA_ORACLE_HOME\fin\fa\apm\oracle\apps\apm\fin\fa\rgx\template
```

Example of the importMetadata command:

```
(UNIX)
importMetadata(application='oracle.security.apm', server='AdminServer',
fromLocation='FA_ORACLE_HOME/fin/fa/apm',
docs='/oracle/apps/apm/fin/fa/rgx/template/FinancialAssetBook.xml'
```

```
(Windows)
importMetadata(application='oracle.security.apm', server='AdminServer',
fromLocation='FA_ORACLE_HOME\\fin\\fa\\apm',
docs='/oracle/apps/apm/fin/fa/rgx/template/FinancialAssetBook.xml'
```

Example 4–2   Importing multiple XML files in one command by using a wild card in the docs parameter

The XML file for data role generation is located in this directory:

```
(UNIX)
/net/machine1/oracle/apps/oracle/fin/gl/rgx/template/GeneralLedger.xml
```

```
(Windows)
\\machine1\oracle\apps\oracle\fin\gl\rgx\template\GeneralLedger.xml
```

The XML file for data security policies generation is located in this directory:

```
(UNIX)
/net/machine1/oracle/apps/oracle/fin/gl/rgx/dataSecPolicy/fndDataSecProvide
r/GeneralLedger.xml
```

```
(Windows)\\machine1\oracle\apps\oracle\fin\gl\rgx\dataSecPolicy\fndDataSecP
rovider\GeneralLedger.xml
```

The following command imports both XML files at the same time:

```
(UNIX) importMetadata(application='oracle.security.apm',
server='AdminServer',
fromLocation='/net/machine1', docs='/oracle/apps/oracle/fin/gl/**'
```

```
(Windows) importMetadata(application='oracle.security.apm',
```

```
server='AdminServer',
fromLocation='\\machine1', docs='/oracle/apps/oracle/fin/gl/**'
```

For more information, see "Importing WebCenter Services Metadata and Data (WebCenter Portal Applications)" in the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter.*

6. If there are any errors in Step 5, follow these steps to recover by restoring the data role templates. Proceed to Step 7 if there are no errors in Step 5.

   a. Promote the MDS label created in Step 4 using the following command:

   ```
   promoteMetadataLabel(application, server, name)
   ```

   The following example promotes the metadata label `data_role_save_point` to the `oracle.security.apm` application deployed in the Administration Server:

   ```
   promoteMetadataLabel('oracle.security.apm', 'AdminServer','data_role_save_
   point')
   ```

   For more information, see "promoteMetadataLabel" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference.*

   b. Delete any new data role templates that were delivered in the patch, using the following command:

   ```
   deleteMetadataLabel(application, server, name)
   ```

   The following example deletes the data role templates in the metadata label `data_role_save_point` from the `oracle.security.apm` application deployed in the Administration Server:

   ```
   deleteMetadataLabel('oracle.security.apm','AdminServer','data_role_save_
   point')
   ```

7. Assuming Steps 3 through 5 are successful, Oracle recommends that you preview the execution of your changed data role templates. Run the preview from the **Summary** tab after you open the data role template from the APM console. For more information, see "Running a Template" in the *Oracle Fusion Middleware Oracle Authorization Policy Manager Administrator's Guide (Oracle Fusion Applications Edition).*

   If the preview results are not correct, follow the recovery described in Step 6 to restore the data role templates. Otherwise, proceed to Step 8.

8. Run the changed data role template and confirm that the data roles and grants are generated correctly. Use the APM role templates summary for reconciliation of the generated artifacts. For more information, see "Running a Template" in the *Oracle Fusion Middleware Oracle Authorization Policy Manager Administrator's Guide.*

9. If all steps are successful, delete the MDS label you created in Step 4, using the `deleteMetaDataLabels` command:

   ```
   deleteMetadataLabel(application, server, name)
   ```

   The following example deletes the metadata label `data_role_save_point` from the `oracle.security.apm` application deployed in the Administration Server:

   ```
   deleteMetadataLabel('oracle.security.apm','AdminServer','data_role_save_point')
   ```

4.17.4 Patching Data Security Grants and Data Role (RGX) Templates

Oracle recommends that you patch data security grants in online mode. Follow the steps in this section when a patch contains both data security grants and data role templates. Every data role template consists of two XML files. One is for data role generation and the other XML file is for data security policies generation. Both of these files must be manually deployed after you apply a patch, so they remain synchronized with each other.

To patch data security grants and data role templates:

1. Run the Patch Impact report to see which artifacts are included in the patch. For more information, see Section 3.5.1, "Patch Impact Report". Note that the Patch Impact report refers to data role templates as `RGXTEMPLATE`.

2. Back up the security store by using the Oracle Database data pump export tool, as described in Section 4.17.5, "Backing up the Data Security Store".

3. The following must be running when patching data security grants and data role templates:

   ■ OPSS Security Store

   ■ Administration Server

   ■ Oracle Authorization Policy Manager

   ■ Database

4. Run Oracle Fusion Applications Patch Manager to apply the seed data changes to the data security system and to copy the data role templates to `FA_ORACLE_HOME`. For more information, see Section 3.4, "Applying Patches".

   When data security changes are introduced in a patch, no manual steps are required in online mode to update the data security subsystem with the GUIDs of the new application roles seeded in the policy story. In offline patching mode or in the case of patch failure, you must manually run the `DSDataMigrator` utility as described in "Reconciling GUIDs" in the *Oracle Fusion Applications Administrator's Guide*.

5. If there are any database errors during Step 4, such as running out of tablespace, fix the database errors that occurred and restart the patch. For general troubleshooting information, see Section 11.5, "Troubleshooting Patching Sessions for Database Content".

   If you are unable to resolve the errors that occurred while applying the seed data changes, recover the seed data from the backup export file you created in Step 2. For more information, see Section 4.17.6, "Recovering Data Security Seed Data from the Backup".

6. To create a save point before deploying the data role templates, use the `createMetadataLabel` WLST command to label the MDS partition for `oracle.security.apm`, using the following syntax:

   ```
   createMetadataLabel(application, server, name)
   ```

   The following example creates the label `data_role_save_point` for the application `oracle.security.apm` deployed in the Administration Server:

   ```
   createMetadataLabel('oracle.security.apm', 'AdminServer', data_role_save_
   point')
   ```

For more information, see "createMetadataLabel" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

7. Follow these steps to manually deploy the data role templates using the `importMetadata` WLST command against the Administration Server in the Common Domain for the `oracle.security.apm` application:

   a. Access the WLST shell.

   ```
   (UNIX) SOA_ORACLE_HOME/common/bin/wlst.sh
   (Windows) SOA_ORACLE_HOME\common\bin\wlst.cmd
   ```

   b. Connect to WebLogic Server.

   ```
   > connect ('admin user name','admin user password','URL of the
   AdminServer')
   ```

   c. Deploy the data role template using the following `importMetadata` WLST command. Refer to the Diagnostics report to find the directory where the template was copied. For more information, see Section 3.5.5, "Diagnostics Report".

   ```
   importMetadata(application='oracle.security.apm', server='Name of
   AdminServer',
   fromLocation='Directory in FA_ORACLE_HOME where data role templates were
   copied',
   docs='Path to the changed data role templates starting with APM partition')
   ```

   Table 4–5 displays the parameters required by the `importMetadata` command.

Table 4–5   Parameters for the importMetadata WLST Command

Parameter Name	Description
application	Enter the value of `oracle.security.apm`
server	Enter the name of your Administration Server
fromLocation	Enter the absolute path to the directory in *FA_ORACLE_HOME* where the patch copied the data role templates. The path must not include the APM partition, because the APM partition is included in the next parameter, `docs`. The Diagnostics report provides the full path and file name in *FA_ORACLE_HOME* for each data role template that was copied from the patch.
docs	Enter the directory for the APM partition, starting with `/oracle/apps/apm`, followed by the remainder of the path, which includes the data role template itself.

Example 4–3   Importing the FinancialAssetBook.xml data role template

In this example, the `FinancialAssetBook.xml` data role template is located in this directory:

```
(UNIX)FA_ORACLE_HOME/fin/fa/apm/oracle/apps/apm/fin/fa/rgx/template
```

```
(Windows)FA_ORACLE_HOME\fin\fa\apm\oracle\apps\apm\fin\fa\rgx\template
```

Example of the `importMetadata` command:

```
(UNIX)
importMetadata(application='oracle.security.apm', server='AdminServer',
fromLocation='FA_ORACLE_HOME/fin/fa/apm',
docs='/oracle/apps/apm/fin/fa/rgx/template/FinancialAssetBook.xml'
```

```
(Windows)
```

```
importMetadata(application='oracle.security.apm', server='AdminServer',
fromLocation='FA_ORACLE_HOME\fin\fa\apm',
docs='/oracle/apps/apm/fin/fa/rgx/template/FinancialAssetBook.xml'
```

Example 4–4   *Importing multiple XML files in one command by using a wild card in the docs parameter*

The XML file for data role generation is located in this directory:

```
(UNIX)
/net/machine1/oracle/apps/oracle/fin/gl/rgx/template/GeneralLedger.xml

(Windows)
\machine1\oracle\apps\oracle\fin\gl\rgx\template\GeneralLedger.xml
```

The XML file for data security policies generation is located in this directory:

```
(UNIX)
/net/machine1/oracle/apps/oracle/fin/gl/rgx/dataSecPolicy/fndDataSecProvide
r/GeneralLedger.xml

(Windows)\machine1\oracle\apps\oracle\fin\gl\rgx\dataSecPolicy\fndDataSecPr
ovider\GeneralLedger.xml
```

The following command imports both XML files at the same time:

```
(UNIX) importMetadata(application='oracle.security.apm',
server='AdminServer',
fromLocation='/net/machine1', docs='/oracle/apps/oracle/fin/gl/**'

(Windows) importMetadata(application='oracle.security.apm',
server='AdminServer',
fromLocation='\\machine1', docs='/oracle/apps/oracle/fin/gl/**'
```

For more information, see "Importing WebCenter Services Metadata and Data (WebCenter Portal Applications)" in the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter.*

8. If there are any errors in Step 7, follow these steps to recover by restoring the data role templates. Otherwise, proceed to Step 9.

   a. Restore the security seed data from the backup you created in Step 2. For more information, see Section 4.17.6, "Recovering Data Security Seed Data from the Backup".

   b. Promote the MDS label created in Step 6 using the following command:

   ```
   promoteMetadataLabel(application, server, name)
   ```

   The following example promotes the metadata label `data_role_save_point` to the `oracle.security.apm` application deployed in the Administration Server:

   ```
   promoteMetadataLabel('oracle.security.apm', 'AdminServer','data_role_save_
   point')
   ```

   For more information, see "promoteMetadataLabel" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

   c. Delete any new data role templates that were delivered in the patch, using the following command:

```
deleteMetadataLabel(application, server, name)
```

The following example deletes the data role templates in the metadata label `data_role_save_point` from the `oracle.security.apm` application deployed in the Administration Server:

```
deleteMetadataLabel('oracle.security.apm','AdminServer','data_role_save_
point')
```

9. Assuming Steps 2 through 7 are successful, Oracle recommends that you preview the execution of your changed data role templates. Run the preview from the **Summary** tab after you open the data role template from the APM console. For more information, see "Running a Template" in the *Oracle Fusion Middleware Oracle Authorization Policy Manager Administrator's Guide (Oracle Fusion Applications Edition)*.

    If the preview results are not correct, follow the recovery described in Step 8 to restore the seed grants and data role templates. Otherwise, proceed to Step 10.

10. Run the changed data role template and confirm that the data roles and grants are generated correctly. Use the APM role templates summary for reconciliation of the generated artifacts. For more information, see "Running a Template" in the *Oracle Fusion Middleware Oracle Authorization Policy Manager Administrator's Guide (Oracle Fusion Applications Edition)*.

    If the results are not correct, restore the database from the backup created in Step 2. For more information, see Section 4.17.6, "Recovering Data Security Seed Data from the Backup".

11. If all steps are successful, delete the MDS label you created in Step 6, using the `deleteMetaDataLabels` command:

```
deleteMetadataLabel(application, server, name)
```

The following example deletes the metadata label `data_role_save_point` from the `oracle.security.apm` application deployed in the Administration Server:

```
deleteMetadataLabel('oracle.security.apm','AdminServer','data_role_save_point')
```

4.17.5 Backing up the Data Security Store

Back up the data security store by using the Oracle Database data pump export tool. Before running the export tool, ensure that the `TWO_TASK` environment variable is set to point to your Oracle Fusion Applications instance. You are prompted for the Oracle Fusion Applications database user name and password.

1. For setting any environment variable, run the `adsetenv` script to generate the `APPSORA.env` file, which when sourced, sets all environment variables.

```
(UNIX)
sh adsetenv.sh
source APPSORA.env
echo $TWO_TASK

(Windows, TWO_TASK is known as LOCAL)
adsetenv.cmd
APPSORA.cmd
echo %LOCAL%
```

2. Run the data pump export tool as follows:

```
ORACLE_HOME/bin/expdp directory=tmp dumpfile=fndds1.dmp tables='(FND_GRANTS,
FND_MENUS_TL,FND_MENUS,FND_MENU_ENTRIES,FND_COMPILED_MENU_FUNCTIONS,
FND_FORM_FUNCTIONS_TL,FND_FORM_FUNCTIONS,FND_OBJECT_INSTANCE_SETS_TL,
FND_OBJECT_INSTANCE_SETS,FND_OBJECTS_TL,FND_OBJECTS)' NOLOGFILE=y
```

For more information about Oracle Data Pump, see:
http://www.oracle.com/technetwork/database/enterprise-edition/data-pump-o
verview-084963.html

4.17.6 Recovering Data Security Seed Data from the Backup

Follow these steps only if a data security seed data patch failed and there is no way to resolve the failure and reapply the patch:

1. Remove the existing data security grant data from the data security tables. Connect to the `fusion` account using SQL*Plus and run the following commands:

```
truncate table fusion.fnd_objects;
truncate table fusion.fnd_objects_tl;
truncate table fusion.fnd_object_instance_sets;
truncate table fusion.fnd_object_instance_sets_tl;
truncate table fusion.fnd_form_functions;
truncate table fusion.fnd_form_functions_tl;
truncate table fusion.fnd_menus;
truncate table fusion.fnd_menus_tl;
truncate table fusion.fnd_menu_entries;
truncate table fusion.fnd_grants;
```

2. Import the data security seed data from the backup export file you previously created.

```
ORACLE_HOME/bin/impdp dumpfile=fndds1.dmp tables='(FND_GRANTS,
FND_MENUS_TL,FND_MENUS,FND_MENU_ENTRIES,FND_COMPILED_MENU_FUNCTIONS,
FND_FORM_FUNCTIONS_TL,FND_FORM_FUNCTIONS,FND_OBJECT_INSTANCE_SETS_TL,
FND_OBJECT_INSTANCE_SETS,FND_OBJECTS_TL,FND_OBJECTS)'
NOLOGFILE=y
```

4.18 Patching Service-Oriented Architecture (SOA) Composites

When updates to SOA composites are introduced in a patch, no manual steps are required if *both* of the following conditions are met:

- You have no SOA composite customizations in Oracle JDeveloper. If you do have customizations, follow the steps in Section 4.18.1, "Preserving SOA Composite JDeveloper Customizations Before Applying a Patch".

- You apply the patch in online mode and no validation or deployment errors occurred during the application of the patch that contains SOA composites. Oracle recommends you do not use offline mode when a patch contains SOA composites. If the patch fails while attempting to deploy a SOA composite, you may have to manually deploy the composite. For more information, see Section 4.18.2, "Manually Deploying SOA Composites".

For information about resolving validation errors, see Section 11.4.2, "Troubleshooting SOA Composite Validation Failures". For information about recovering from deployment errors, see Section 11.4.3, "Troubleshooting SOA Composite Deployment Failures".

If you customized SOA composites used by Oracle Fusion Applications in JDeveloper, you must preserve these customizations before you apply a patch that includes the next revision of the composite. Other customizations to the SOA composite being patched are automatically merged by the SOA deployment command called during patching. These runtime customizations, such as design time and run-time (DT@RT) changes or property changes, do not require a manual merge process.

What must be running when you patch SOA composites

■ Administration Server

■ SOA-INFRA Managed Servers

■ Database

■ At least one server must be running the Policy Manager component from the Web Services Manager (WSM-PM) application. Typically in an Oracle Fusion Applications environment, this is the Common Cluster, for example in the `CRMDomain`, it is the `CRMCommonCluster`. You can find out which server is running by logging in to Oracle Enterprise Manager Fusion Applications Control to verify that the application named `wsm-pm` is running with an `OK` or **green** status. If the server is not running, see "Diagnosing Common Problems with Oracle WSM" in the *Oracle Fusion Middleware Security and Administrator's Guide for Web Services*.

4.18.1 Preserving SOA Composite JDeveloper Customizations Before Applying a Patch

If you performed JDeveloper customizations, not supported by OPatch, to a SOA composite and then you deploy the composite to the SOA runtime, subsequent patches are not directly deployable. The Oracle Fusion Applications Patch Manager validation process returns the appropriate error, which instructs you to take the newer version of the composite that is in the patch, redo the same customizations that were performed on the previous version of the composite, and then apply the patch in online mode to deploy the composite.

Before applying the patch, review the recommendations in "Merging Runtime Customizations from a Previously Deployed Revision into a New Revision" in the *Oracle Fusion Applications Extensibility Guide* to ensure that your customizations will be merged successfully.

To preserve SOA composite JDeveloper customizations before applying a patch:

1. Run Oracle Fusion Applications Patch Manager validation in online mode to determine which composites have JDeveloper customizations. If any customizations are detected, the validation results display the SOA composite name, its location in the `patch_top` directory, and the requirement for you to merge JDeveloper customizations into the `sca_*.jar` file in the `patch_top` directory before applying the patch in online mode. For more information, see Section 3.3, "Validating Patches".

   > **Note:** You must run Oracle Fusion Applications Patch Manager validation before applying every patch, especially patches that contain SOA composites. If your JDeveloper customizations are not merged into the `sca_*.jar` file in the `patch_top` directory, the deployment of the SOA composite that was changed inside the patch will fail when you apply the patch.

2. Open the custom SOA workspace and the customized version of the Fusion Applications SOA composite in JDeveloper using "Oracle Fusion Applications Developer". For more information, see "Customizing SOA Composites with JDeveloper" in the *Oracle Fusion Applications Web User Interface Developer's Guide for Oracle Application Development Framework*.

3. Import the composite `sca_*.jar` file from the `patch_top` directory into the project, for example revision `yy_patchnum`, in JDeveloper. Make note of this revision number in the deployment window because you will need it in Step 8. You can find the revision number on the Patch Impact report.

4. Restart JDeveloper in the Oracle Fusion Applications Administrator Customization role.

5. Verify that there are no errors in JDeveloper.

6. Verify that the changes introduced in both the customized version and the patched version are present.

7. Right-click the composite project in the Application Navigator, select **Deploy**, select the composite, click **Deploy to SAR**, and click **Next**.

8. Manually change the value in **New Revision ID** to the revision from Step 3, for example, `yy_patchnum`, and click **Finish**.

9. If the deployment folder is set to a location different from that of the `patch_top` directory, copy and replace the JAR in the patch under *patch_top*/patch_ mw/files/*productfamily*/deploy. If your file name is different, rename it to the original name.

10. Now you should be able to both validate and apply this patch successfully using Oracle Fusion Applications Patch Manager in online mode.

For more information about customizing SOA composites, see "Customizing and Extending SOA Components" in the *Oracle Fusion Applications Extensibility Guide*.

4.18.2 Manually Deploying SOA Composites

If a customized SOA composite deployment fails during patching, you must manually deploy this composite using WLST commands. You must also manually deploy SOA composites if you apply a patch in offline mode that contains SOA composites.

To apply a SOA composite manually after a deployment failure or when patching in offline mode

In the following steps, the example composite `FinAp` is patched from revision 1.0 to revision 2.0 and the SAR file of revision 2.0 is in *FA_ORACLE_ HOME*/crm/deploy/sca_FinAp_rev2.0.jar.

Note that the parameters are for illustration purposes only.

1. Refer to the Diagnostics report to find the name and location of the `sca_*.jar` file that was copied to *FA_ORACLE_HOME* by Oracle Fusion Applications Patch Manager. For more information, see Section 3.5.5, "Diagnostics Report".

2. If the previous revision contained JDeveloper customizations, ensure that you deploy the patched revision with the merged JDeveloper customizations. Using the `sca_*.jar` file from Step 1, follow the JDeveloper customization merge instructions that are described in Section 4.18.1, "Preserving SOA Composite JDeveloper Customizations Before Applying a Patch". Then use the merged sca_ *.jar for Step 3.

3. Deploy the patched composite using single patch composite command.

```
sca_patchComposite('SOA-Infra URL', user, password,
'/FA_ORACLE_HOME/crm/deploy//sca_FinAprev2.0.jar',
mergeLogFile='/tmp/merge-log.txt')
```

4.19 Patching SOAEXTENSION Artifacts

When updates to SOAEXTENSION artifacts are introduced in a patch, you must stop and restart all SOA-INFRA Managed Servers in all domains. Both online and offline patching require this step.

4.20 Patching SOA Resource Bundles

Oracle recommends you patch SOA resource bundles in online mode. No manual steps are required when patching SOA resource bundles in online mode unless the SOA resource bundle JAR file contains translatable strings for human task-mapped attribute labels and standard view names, as indicated by a JAR name that ends with `FlexFieldSoaResource.jar`. In offline mode, in case of patch failure, or if the patch contains human task-mapped attribute labels and standard view names, you must manually deploy the SOA resource bundle and restart the SOA composites that depend on the SOA resource bundle.

The following must be running when you patch SOA resource bundles:

- Administration Server

- SOA-INFRA Managed Servers

- Node manager

- Database

After you apply the patch, refer to the Diagnostics report to get a complete list of composites that depend on each SOA resource bundle and also the domains. For more information, see Section 3.5.5, "Diagnostics Report".

4.20.1 Manually Deploying SOA Resource Bundle JAR Files

1. From the Diagnostics report for patch validation, review the list of SOA resource bundle JAR files included in the patch and the domain where they should be deployed. Use the `ant-sca-deploy.xml` script to deploy the appropriate SOA cluster for each JAR included in the patch.

   Set the `ANT_HOME` variable:

   ```
   ANT_HOME=FA_ORACLE_HOME/modules/org.apache.ant_1.7.1; export ANT_HOME
   ```

   Deploy the appropriate cluster:

   ```
   ant -f Middleware_Home/SOA_Suite_Home/bin/ant-sca-deploy.xml
       -DserverURL=URL_to_SOA_server
       -DsarLocation=Location_of_resource_bundle_jar under FA_ORACLE_HOME
       -Duser=weblogic
       -Dpassword=weblogic_password
   ```

   For more information about the `ant-sca-deploy.xml` script that is used to deploy the SOA resource bundle, see "How to Manage SOA Composite Applications with ant Scripts" in the *Oracle Fusion Middleware Developer's Guide for Oracle SOA Suite*.

2. The Diagnostics report lists the composite affected by the patch and the domain where the composite is deployed. Follow these steps for each affected composite:

   a. Log in to Oracle Enterprise Manager Fusion Applications Control in the domain where the composite is deployed.

   b. Go to *domain name,* then **SOA**, then *soa-infra* (SOA cluster name), then **default**, and then *composite name.*

   c. Click **Shut Down**.

   d. Click **Yes** in the confirmation window.

   e. Click **Start Up**.

   f. Click **Yes** in the confirmation window.

3. Review the list of SOA resource bundle JAR files being patched. If a patch contains a JAR file with a name which starts with "jar_" and ends with "FlexFieldSoaResource.jar", for example, `jar_AppCmmnCompNotesFlexFieldSoaResource.jar`, you must perform the following steps to ensure that the patched resource bundle is reflected in the Oracle BPM Worklist. These steps describe how to set the `WorkflowCustomClasspathURL` MBean property to null, and then set it to `oramds:///apps/resource/` and apply the changes in Oracle Fusion Applications Control.

   a. Log in to Oracle Fusion Applications Control in the domain where the JAR was deployed.

   b. Go to **SOA**, then **soa-infra** in the left-hand panel. Go to **SOA Infrastructure**, then **Administration**, and then **System MBean Browser** in the right-hand panel.

   c. Go to **Application Defined MBeans**, then **oracle.as.soainfra.config**, then **Server:** *SOA cluster name*, then **WorkflowConfig** and then **human-workflow**.

   d. Remove the contents in the **Value** column of the `WorkflowCustomClasspathURL` attribute.

   e. Click **Apply**.

   f. Enter `oramds:///apps/resource/` in the **Value** column of the `WorkflowCustomClasspathURL` attribute.

   g. Click **Apply**.

For information about shutting down and starting up SOA composites in Oracle Enterprise Manager, see "Managing the State of Deployed SOA Composite Applications" in the *Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite and Oracle Business Process Management Suite*.

4.21 Patching Sales Prediction Engine (SPE) Inline Service Artifacts

Oracle recommends that you patch data role templates in online mode. When updates to SPE Inline Service artifacts are introduced in a patch, no manual steps are required in online mode to deploy the changed SPE artifacts.

Updates to SPE Inline Service are delivered in the `SPE_ILS.zip` file and the `AdfZspPredictionModuleSupportUtilities.jar` file. This section contains information about manual deployment of SPE artifacts, in the case of offline patching or failure during online patching.

- Prerequisites Required Before Manual SPE Artifact Deployment
- Manually Deploying SPE Artifacts After You Apply the Patch in Offline Mode

> **Note:** SPE artifacts are provisioned only when Oracle Fusion CRM Performance Management is provisioned. If CRM Performance Management is not provisioned in your environment, you should not deploy SPE artifacts.

4.21.1 Prerequisites Required Before Manual SPE Artifact Deployment

1. You must be running JDK 1.6 or later.

2. You must have access to the ZIP file, `rtd-deploytool-11.1.1.zip`. This ZIP file resides inside another ZIP file, *FA_ORACLE_HOME*`/bi/clients/rtd/rtd_client_11.1.1.zip`.

3. Make a backup copy, in a temporary directory, of the existing `SPE_ILS.zip` file, which is located under *FA_ORACLE_HOME* in this directory:

   (Unix)
   ```
   crm/components/crmPerformance/zsp/predictionmodule/inlineservice
   ```

   (Windows)
   ```
   crm\components\crmPerformance\zsp\predictionmodule\inlineservice
   ```

4.21.2 Manually Deploying SPE Artifacts After You Apply the Patch in Offline Mode

Oracle suggests you refer to the text file that was created when provisioning completed, which is a textual overview of your topology, as you follow these steps. For more information, see "Installation Process Flow" in the *Oracle Fusion Applications Installation Guide*.

1. Stop and start `bi_server1` to include the changes in `AdfZspPredictionModuleSupportUtilities.jar`.

2. Follow these steps to deploy the new `SPE_ILS`.zip artifact.

   a. Unzip `rtd_client_11.1.1.zip` in a temporary directory. To find this file, refer to Step 2 in Section 4.21.1, "Prerequisites Required Before Manual SPE Artifact Deployment".

   b. In the unzipped files, go to the folder `.../client/CommandLineDeploy` and find `rtd-deploytool-11.1.1.zip`.

   c. Unzip `rtd-deploytool-11.1.1.zip` and go to the folder, `.../OracleBI/RTD/deploytool`.

   d. In this folder, open a command terminal. Ensure that you have the JDK class path set for this terminal.

   e. Run this command:

   ```
   java -jar deploytool.jar -deploy
   -server Host name of the server where BI domain is created
   -port Managed server port where the OracleRTD app is deployed
   -terminateSessions true Full directory path to SPE_ILS.zip
   ```

   Example:

```
(UNIX) java -jar deploytool.jar -deploy -server server01.oracle.com -port
7001 -terminateSessions true FA_ORACLE_HOME/crm/components/ \
crmPerformance/zsp/predictionmodule/inlineservice/SPE_ILS.zip

(Windows) java -jar deploytool.jar -deploy -server server01.oracle.com
 -port 7001 -terminateSessions true D:\SPE\RTD\ILS\SPE_ILS.zip
```

f. When prompted, enter the user name and password to connect to the RTD server. This user must have a role that includes ILS deploy permission. Both the `BIAdministrator` and `BIAuthor` have this permission.

g. This message indicates the deployment is complete:

```
deploymentStateId is 5
Inline service "SPE_ILS" in "FA_ORACLE_
HOME/crm/components/crmPerformance/zsp/predictionmodule/inlineservice/SPE_
ILS.zip/SPE_ILS.zip"
deployed to server: "server01.oracle.com" port: "7001" deployment state:
"Development"
```

4.22 Patching Tree Artifacts

Tree artifacts are delivered as seed data in patches and therefore, do not typically require manual steps after they are patched. A process called *tree flattening* automatically runs during the patching process. If this process fails, you must perform the following additional steps:

1. To verify if the patch contains any files related to tree flattening, refer to the Patch Impact report and look for a file named `FndTreeVersionSD.xml`. This is the only file that requires tree flattening. For more information, see Section 3.5.1, "Patch Impact Report".

2. Confirm that the tree version changes were successfully flattened by reviewing the worker logs for errors related to tree flattening. To determine the worker that executed the specific seed data task, based on the file name FndTreeVersionSD.xml, refer to the Diagnostics report generated at the end of the patching session. Note any tree versions that failed because you need the version numbers to manually flatten the tree version changes.

   For more information about the Diagnostic report, see Section 3.5.5, "Diagnostics Report". For more information about log files, see Section 11.1.1, "Log Files for Patching Sessions".

3. Follow these steps to manually flatten tree versions:

   a. Access the administrative area of Oracle Fusion Functional Setup Manager by logging in to Oracle Fusion Applications with a user account that is provisioned with the necessary role. Contact your security administrator for details.

   b. From the **Administration** menu in the work area of Oracle Fusion Applications, choose **Setup and Maintenance.**

   c. Choose the **Manage Trees and Tree Versions** task.

   d. Search for the tree versions that require flattening.

   e. Choose the appropriate tree version and optionally choose **Audit** from the **Actions** menu to diagnose the issues.

   f. If you want to make changes to the tree version, click the tree version and edit it.

g. Choose **Flattening**, **Row Flattening**, then **Flattening, Column Flattening** from the **Actions** menu to flatten the selected tree version.

For more information about trees, see "Define Trees" in the *Oracle Fusion Applications Common Implementation Guide*.

5

Installing Release Update Patches (11.1.3.0.0)

This chapter describes how to install release update patches in Oracle Fusion Applications.

This chapter contains the following topics:

- Introduction to Oracle Fusion Applications Release Update Patches
- Prepare to Install a RUP - Pre-Down Time
- Prepare to Install a RUP - During Downtime
- Install a RUP
- Troubleshoot RUP Installer Sessions

5.1 Introduction to Oracle Fusion Applications Release Update Patches

This section provides an introduction to the following concepts related to release update patches:

- Release Update Patches
- Oracle Fusion Applications RUP Installer (RUP Installer)
- RUP Installer User Interface
- RUP Installer Configuration Tasks

5.1.1 Release Update Patches

A RUP is a set of cumulative patches and changes for the entire Oracle Fusion Applications Suite, for a base release. A RUP can sometimes introduce new functionality, and should be applied when suitable. You install RUPs with Oracle Fusion Applications RUP Installer. To install a certain version of a RUP you must have successfully installed the previous version.

5.1.2 Oracle Fusion Applications RUP Installer (RUP Installer)

RUP Installer is a Java-based installer that enables you to install a group of patches across all product families, to upgrade Oracle Fusion Applications to the next release. RUP Installer can patch existing content and can also copy and deploy new artifacts, depending on the contents of the RUP. You run RUP Installer in interactive mode and proceed through the installation by providing information in the user interface when prompted.

5.1.3 RUP Installer User Interface

RUP Installer provides a graphical user interface which allows you to control the behavior of the installer by the use of buttons, in cases where it encounters a failure. Note that the behavior of these buttons may vary, depending on whether it is a task, or a step within a task, that fails. The behavior also depends on whether a task is mandatory. All mandatory configuration tasks must complete successfully before proceeding to the next configuration task. For information about which tasks are mandatory, see Section 5.1.4, "RUP Installer Configuration Tasks".

You can exit RUP Installer in the event of a failure and restart from the point of failure. If a non-mandatory task fails, and you continue to the next task, you must restart RUP Installer after it completes with incomplete tasks. When you restart, RUP Installer retries all failed configuration tasks and steps. For more information about what to do when a configuration action fails, see Section 5.5.3, "General Troubleshooting During the Configuration Phase".

An explanation of the usage of each button follows.

5.1.3.1 Abort Button

The **Abort** button allows you to skip a failed task or step within a task, and records the failure so it can be rerun when you restart the installation. For mandatory tasks, after you abort the task, RUP Installer does not proceed and only the **Cancel** button is enabled. You must then resolve the cause of the failure and start RUP Installer from this failure point. For non-mandatory tasks, RUP Installer proceeds to the next configuration task after you abort the task. This button is enabled only after a failure.

5.1.3.2 Cancel Button

The **Cancel** button allows you to stop a RUP Installer session after a failure. This button is enabled only after a failure.

5.1.3.3 Close Button

The Windows **Close** button allows you to stop a RUP Installer session after a failure. This button is enabled only after a failure.

5.1.3.4 Continue Button

The **Continue** button allows you to skip a failed step within a task that is not mandatory, or a non-mandatory task, and records the failure. RUP Installer then proceeds with the next step. When you rerun this RUP Installer session, the failed configuration actions are attempted again.

Note that this button is enabled only for configuration tasks that contain steps and is not enabled in the case of failure for configuration tasks that do not contain steps.

5.1.3.5 Next Button

The **Next** button allows you to proceed to the next screen. This button is enabled only when all tasks complete successfully in the current screen.

5.1.3.6 Retry Button

The **Retry** button allows you to attempt to run a failed configuration task, or a step within a task, again. Use **Retry** when you know the cause of the failure and can resolve the issue during the current RUP Installer session.

5.1.4 RUP Installer Configuration Tasks

During the installation phase, RUP Installer copies all files from the RUP to the appropriate location, such as Oracle Fusion Middleware home and Oracle Fusion Applications Oracle home. After the file copy is completed, RUP Installer performs the Policy Store Analysis, as described in Table 5–4. Upon successful completion of the Policy Store Analysis, RUP Installer calls Configuration Assistants to perform the remaining tasks required to update and deploy the artifacts included in the RUP. Depending on the contents of the RUP, not all tasks run.

If any tasks fail during the installation phase, refer to Section 5.5.2, "Troubleshooting Failures During the Installation Phase".

All mandatory configuration tasks must complete successfully before proceeding to the next configuration task. For more information, see Section 5.5.3, "General Troubleshooting During the Configuration Phase".

Table 5–1 provides a complete list of possible configuration tasks. The Retry Behavior column describes what RUP Installer does after a configuration task fails and you use the **Retry** button. If available, links are provided to the relevant troubleshooting sections.

Table 5–1   Configuration Tasks Run by Oracle Fusion Applications 11g Release 1 (11.1.3.0.0) RUP Installer

Name	Mandatory	Description	Retry Behavior
Configure Patch Manager	Yes	Configures Oracle Fusion Applications Patch Manager	Starts from the beginning of the task
Bootstrap Patch Manager	Yes	Updates the data model for Oracle Fusion Applications Patch Manager by running the fapmgr `bootstrap` command.	Starts from the beginning of the task See Section 5.5.6, "Error During Bootstrapping Patch Manager".
Verify Middleware PSA Schema Credentials	Yes	Verifies users and logins for schema.	Starts from the beginning of the task.
Apply Middleware Patch Sets	Yes	Applies Oracle Fusion Middleware patch sets, which include schema changes and installers.	Starts from the beginning of the task. See Section 5.5.8, "Failure During Applying Middleware Patch Sets".
Apply Pre-PSA Middleware Patches	Yes	Applies WebLogic Server Smart Update patches and Opatch based patches. See Section 5.1.4.1, "Installers Invoked by the Apply Pre-PSA Middleware Patches Tasks" and Section 5.1.4.2, "Patches Not Supported by the Apply Pre- and Post-PSA Middleware Patches Tasks".	Applies the failed patches. See Section 5.5.7, "Troubleshooting Applying Middleware Patches".
Upgrade Middleware Schemas	Yes	Runs Oracle Fusion Middleware patch sets assistants.	Starts from the beginning of the task.

Table 5–1 (Cont.) Configuration Tasks Run by Oracle Fusion Applications 11g Release 1 (11.1.3.0.0) RUP Installer

Name	Mandatory	Description	Retry Behavior
Apply Post-PSA Middleware Patches	Yes	Applies patches that update Oracle Fusion Middleware Extensions for Applications objects. See Section 5.1.4.2, "Patches Not Supported by the Apply Pre- and Post-PSA Middleware Patches Tasks"	Applies the failed patches. Section 5.5.7, "Troubleshooting Applying Middleware Patches".
Offline Preverification	Yes	Performs the following validation checks while all servers are shutdown: ■ Policy Store ■ Number of database workers ■ Database Content Upload ■ Business Process Management (BPM) Template ■ Oracle Data Integrator (ODI)	Runs failed steps Section 5.5.11, "LdapServerCheck Failure".
Load Database Components	Yes	Uploads the database content packaged in the RUP to the database, such as database objects, seed data, and package headers and bodies.	Runs failed database commands. See Section 5.5.10, "Troubleshooting Loading Database Components".
Upgrade OPSS	Yes	Upgrades the OPSS DIT and schema in the security store. Upgrades the configuration on each domain. Adds Delegated Administration policies to the policies in the security store.	Starts from the beginning of the task. See Section 5.5.11, "LdapServerCheck Failure".
Deploy Applications Policies (jazn-data.xml)	Yes	Performs the deployment of the updated applications policies, based on your selections during the Policy Store Analysis task. This task does not run if you installed a Language Pack and chose to override the base English strings in the policy store by using the `J-DupdateJAZNPolicyStore` option set to true.	Deploys the failed stripes. See Section 5.5.12, "Troubleshooting Deployment of Applications Policies".
Deploy Data Security Grants	Yes	Performs GUID reconciliation in LDAP.	Starts from the beginning of the task.
Generate ADF Domain Configuration Plan	Yes	Generates Oracle ADF domain configuration in Metadata Service (MDS) to be used by Expression Language (EL) expressions in `connections.xml`.	Starts from the beginning of the task.
Generate ESS Connections File	Yes	Generates `adf-domain-config.xml` in MDS to be used by EL expressions in ESS `connections.xml`.	Starts from the beginning of the task.
Generate SOA Configuration Plan	Yes	Generates the configuration plan to be used for deploying SOA composites.	Starts from the beginning of the task.
Update Flexfield Configuration	Yes	Updates the required configuration file for supporting new flexfields, new flexfield usages, and flexfield view links added by Oracle Fusion Application products.	Starts from the beginning of the task.

Table 5–1 (Cont.) Configuration Tasks Run by Oracle Fusion Applications 11g Release 1 (11.1.3.0.0) RUP Installer

Name	Mandatory	Description	Retry Behavior
Deploy BPM Templates	Yes	Deploys BPM Templates to the MDS repository.	Deploys failed templates.
Deploy BI Publisher Artifacts	Yes	Deploy Copies captions and deploys Webcat to the Oracle Business Intelligence repository using Catalog Manager.	Starts from the beginning of the task. See Section 5.5.15, "Failure During Deployment of BI Publisher Artifacts".
Import Oracle Data Integrator Repository	Yes	Imports ODI related changes to the ODI repository.	Imports failed data.
Apply Offline Setting Changes	Yes	Applies Oracle Fusion Applications environment configuration setting changes during the offline phase.	Starts from the beginning of the task.
Verify Node Manager and OPMN Status	Yes	Checks for access to the Node Manager and the Oracle Process Manager and Notification Server (OPMN) control process, and should fail because you manually shut these processes down prior to starting RUP Installer. You must manually start both the Node Manager for all domains and the OPMN control process at this time. You must not exit out of RUP Installer during this task.	Runs failed steps.
Start all servers	No	Starts all servers in all domains, including the BI servers.	Restarts failed servers. See Section 5.5.16, "Failures During Starting All Servers"
Online Preverification	Yes	For more information, see Section 5.1.4.3, "Validation Steps Performed During Online Preverification Task".	Runs failed steps. See Section 5.5.9, "EditTimedOutException Error During Online Preverification" and Section 5.5.18, "Merging SOA Composite JDeveloper Customizations While Installing a RUP".
Generate OHS Reference Configuration File	No	Generates Oracle HTTP Server (OHS) configuration files for installed product families in this directory: `APPLICATIONS_BASE`/fusionapps/applications/admin/OHS/patched_moduleconf. You must manually modify the related properties file in order for this task to be successful. For more information, see Section 5.2.12, "Update Oracle Fusion Middleware Schema Credentials".	Starts from the beginning of the task.

Table 5–1 (Cont.) Configuration Tasks Run by Oracle Fusion Applications 11g Release 1 (11.1.3.0.0) RUP Installer

Name	Mandatory	Description	Retry Behavior
Apply OAM Configuration	No	Applies changes to the Oracle Access Manager configuration. You must manually modify the related properties file in order for this task to be successful. For more information, see Section 5.2.12, "Update Oracle Fusion Middleware Schema Credentials".	Starts from the beginning of the task. See Section 5.5.13, "Failure during Applying OAM Configuration".
Deploy Flexfields	No	Deploys flexfields to the domain that hosts the `FndSetup` application.	Starts from the beginning of the task.
Import Image Routing (IPM) Artifacts	No	Deploys IPM artifacts to the IPM server.	Retries only failed IPM artifacts. See Section 5.5.17, "Failure During IPM Import".
Deploy B2B Metadata	No	Deploys B2B Metadata.	Deploys failed B2B artifacts.
Deploy SPE Inline Service Artifacts	No	Deploys SPE Inline Service Artifacts.	Retries the deployment.
Deploy Data Role (RGX) Templates	No	Deploys RGX Template artifacts to the Common Domain.	Deploys failed templates.
Import Group Space Templates	No	Imports Group Space Templates	Deploys failed templates.
Deploy SOA Shared Repository Artifacts	No	Deploys SOA shared repository artifacts to SOA servers available in the environment.	Deploys failed SOA shared repository artifacts.
Deploy SOA Composites	No	Deploys SOA composites to the corresponding SOA servers and performs server management steps.	Deploys failed SOA composites. See Section 5.5.19, "Troubleshooting SOA Composite Deployment Failures".
Deploy SOA Resource Bundles	Yes	Deploys SOA Resource Bundles to the corresponding SOA servers.	Deploys failed SOA resource bundles.
Restart All SOA Servers	No	Restarts all SOA servers in the environment.	Starts at the beginning of the task.
Applying Online Setting Changes	No	Applies Oracle Fusion Applications environment configuration setting changes during the online phase.	Starts from the failed task.
Apply BI Metadata Updates	Yes	Applies Oracle Business Intelligence Metadata Updates.	Applies failed patches.Section 5.5.20, "Failure During Applying BI Metadata Updates".

5.1.4.1 Installers Invoked by the Apply Pre-PSA Middleware Patches Tasks

The following installers are installed by the **Pre-PSA Middleware Patches** configuration task:

- Oracle Business Intelligence

- Oracle Common

- Oracle Data Integrator (ODI)

- Oracle Database Client

- Oracle Enterprise Content Management

- Oracle HTTP Server (OHS) - Note that this is the embedded OHS. OHS may also be installed in the DMZ. Patching OHS in the DMZ is a manual process not supported by RUP Installer.

- Oracle Fusion Middleware Extensions for Applications

- Oracle Global Order Promising

- Oracle Secure Enterprise Search (SES)

- Oracle SOA Suite

- Oracle WebCenter Suite

- Oracle WebLogic Server

- Oracle Web Tier

5.1.4.2 Patches Not Supported by the Apply Pre- and Post-PSA Middleware Patches Tasks

The following patches are not supported by these configuration tasks:

- Patching Integrated Development Environment (IDE)

- Patching OHS installed in the DMZ. For more information, refer to Oracle Fusion Applications release notes for information about mandatory OHS patches.

- Patching your Database Server. For more information, see Section 5.3.2, "Apply Mandatory Prerequisite Patches".

- Patching your Oracle Identity Management Server. For more information, refer to "Oracle Identity Management Patches for Oracle Fusion Applications" in Oracle Fusion Applications release notes.

5.1.4.3 Validation Steps Performed During Online Preverification Task

The following validation steps are performed during this task:

- Taxonomy URL

- Flexfield: Checks if the flexfield deployed Managed Server is up

- OAM Configuration

- SOA Shared Repository: Verifies the taxonomy, checks if the Administration Server is up, and if the SOA platform is ready

- SOA Resource Bundle: Verifies the taxonomy, checks if the Administration Server is up, and if the SOA platform is ready

- SOA Composite: Performs the following validation steps:

  - Verifies the taxonomy

  - Checks if the Administration Server is up

  - Checks if the SOA platform is ready

  - Checks if the base composite is deployed

- Checks if the default revision is deployed

- Checks if the new revision is not deployed

- Checks whether the SOA composites that will be affected by the patch have JDeveloper customizations. For more information, see Section 5.5.18, "Merging SOA Composite JDeveloper Customizations While Installing a RUP".

- Image Routing (IPM): Checks if the IPM server is up

- B2B Metadata: Checks if the Common Domain SOA Managed Server and the LDAP Server are up

- SPE Inline Service: Checks if the Oracle CRM Performance application is deployed. If it is, the OracleRTD application must be deployed and at least one BI server must be running where the OracleRTD application is deployed.

- Data Role (RGX) Template: Checks if the Administration Server for the Common Domain is up

- Group Space Template: Checks if the following Managed Servers are up: `WC_Spaces, WC_Collaboration, ucm_server1`

5.2 Prepare to Install a RUP - Pre-Down Time

This section describes the following preparation steps for installing a RUP, all of which can be performed before your scheduled down time.

- Before You Begin

- Confirm Installation of Oracle Fusion Applications RUP1 (11.1.2.0.0)

- Download the RUP Repository

- Configure Oracle Metadata Services (MDS)

- Verify Your OPatch Version

- Confirm Memory Settings

- Confirm Host Name (Unix)

- Add -d64 Option to JRE_MEMORY_OPTIONS (Solaris X64 and Solaris Sparc)

- Confirm the Local Port Range Value

- Confirm Database Settings

- Confirm All Oracle Homes Are Registered in the Central Inventory

- Update Oracle Fusion Middleware Schema Credentials

- Maintain Versions of Customized BI Publisher Reports

- Confirm That JDeveloper Customizations Can Be Merged

- Verify Credentials in Oracle Directory Services Manager (ODSM)

- Verify the Default Realm Name is myrealm

- Save WebLogic Configuration Changes

5.2.1 Before You Begin

Before you begin the upgrade, you should have access to the following documentation:

- RUP Installer documentation from the previous release

- Oracle Fusion Applications release notes from the previous release

- Oracle Fusion Applications release notes from the release you are upgrading to

You should also have a clear understanding of the following host and directories:

- **Primordial host**: The primordial host is where the Administration Server for the Common Domain runs

- *APPLICATIONS_CONFIG*: The top-level directory for the Oracle Fusion Applications configuration files

- *APPLICATIONS_BASE*: The top-level directory for the Oracle Fusion Applications binaries

- *FA_ORACLE_HOME*: Directory named `applications`, located under the `fusionapps` Oracle Fusion Applications Middleware home

For more information, see "Provisioned Oracle Fusion Applications Home Directories" in the *Oracle Fusion Applications Administrator's Guide*.

5.2.2 Confirm Installation of Oracle Fusion Applications RUP1 (11.1.2.0.0)

Ensure that you have successfully installed RUP1 and followed all post installation tasks in the RUP2 documentation and in the "Applying Patches" section of Oracle Fusion Applications Release Notes. For more information, see Oracle Fusion Applications Release Notes, 11g Release 1, Update 1 (11.1.2.0.0) Document 1382781.1.

5.2.3 Download the RUP Repository

The RUP repository contains RUP Installer and Oracle Fusion Middleware patches that are required to install a RUP in an existing Oracle Fusion Applications environment. You download the repository from the Oracle Fusion Applications Product Media Package to a location of your choice. This directory is referred to as *REPOSITORY_LOCATION*.

5.2.3.1 Obtaining the Software

Oracle groups its software releases by product area. A **Product Media Pack** refers to those groupings. Each media pack may also include a zipped file containing electronic documentation files or "Quick Install" files, which facilitate the initial installation of the software.

Once you have completed the software licensing agreements, you can obtain the Oracle Fusion Applications software using one of these two methods:

- **Oracle Software Delivery Cloud Portal**: Provides you with a readme document that helps you to determine which media you need to fulfill the license you have purchased. You download only the media you need. This is the default delivery method.

- **Oracle Store**: Provides a complete set of the software in DVD format. You use only the DVDs covered by your software licensing agreement.

Using either method, you can obtain the Oracle Fusion Applications RUP repository and gain access to the Oracle Fusion Applications documentation library.

5.2.3.2 Downloading from the Oracle Software Delivery Cloud Portal

Go to http://edelivery.oracle.com/ and follow these instructions:

1. Complete the Export Validation process by entering basic identification information using the online form.

2. On the Media Pack Search page, specify the product pack and platform to identify the media pack you want to download. If you do not know the name of the product pack, you can search for it using the license list.

3. Choose the appropriate media pack from the search results and download the Release Update Patch repository (in zipped format). You can download the repository to a location of your choice.

4. Extract the contents of all zipped files to the same target directory. The directory must be on a networked drive or shared disk so that it will be accessible to all the hosts in your new environment. The installers are normally located in the `installers` subdirectory under *REPOSITORY_LOCATION*.

> **Note:** You should avoid creating the repository in a deeply nested directory on Windows. The Windows PATH variable has a limited size, and long directory names may cause it to overflow. For example, `c:\work\my_repository` is a better choice than `c:\Work\WorkInProgress\FusionApps\FusionAppsv1\Nov2011\tempfiles\my_repository`.

5.2.3.3 Release Update Patch Installers

Table 5–2 lists the installers in the RUP repository.

Table 5–2   RUP Installers

Media Label Name	Staging Destination
RUP Installer	(Unix) *REPOSITORY_LOCATION*/installers/fusionapps/Disk1/runInstaller
	(Windows) *REPOSITORY_LOCATION*\installers\fusionapps\Disk1\setup.exe

5.2.4 Configure Oracle Metadata Services (MDS)

Confirm that DBMS_STATS has recently been run on the MDS schema in the Oracle Fusion Applications database. This step optimizes the performance of starting servers. For more information, see "Collecting Optimizer Statistics" in the *Oracle Fusion Applications Administrator's Guide*.

Then follow the steps in "Configuring Oracle Metadata Services" in the *Oracle Fusion Applications Post-Installation Guide*.

5.2.5 Verify Your OPatch Version

Follow this step only if you have updated OPatch in the *FA_ORACLE_HOME* outside of what Oracle Provisioning and RUP Installer installs.

Oracle Fusion Applications is compatible with a specific version of OPatch instead of the generic version of OPatch. If an incompatible version of OPatch exists in *FA_ORACLE_HOME*, errors can occur while applying patches and running RUP Installer. The compatible version of OPatch is available on My Oracle Support under patch 14044793.

If the file, *FA_ORACLE_HOME*/OPatch/ocm/lib/emocmclnt.jar exists, then you have an incompatible version of OPatch, and you must contact Oracle Support to fix

this issue. On Windows, look for *FA_ORACLE_ HOME*\OPatch\ocm\lib\emocmclnt.jar.

5.2.6 Confirm Memory Settings

Confirm that memory requirements are met on the primordial host that the RUP installer is launched from. The primordial host is where the Administration Server for the Common Domain runs.

RUP Installer requires at least 6GB of free RAM on the 64-bit domains to be up during the installation. RUP installer also requires at least 6GB of free RAM on the 64-bit primordial host that the installer is launched from, for the duration of the RUP installation. This 6GB of free memory requirement is in addition to the memory requirement for all servers, including the Administration Servers on the primordial host that is already up and running. Oracle also recommends at least 1GB of additional free memory on the primordial host during the RUP installation as a safety net.

For example, if the BI domain is provisioned on the primordial host, then RUP Installer requires this 64-bit primordial host to have a minimum of 12GB of RAM. If you have two 64-bit hosts with the BI domain provisioned on a different host from the primordial host, then one host runs the Administration Server and the BI servers, while the other host runs RUP Installer, which requires a connection to the Administration Server that is running. If you run RUP installer and the Administration Server on the same primordial host with insufficient memory, then the Administration Server and Managed Servers may fail.

5.2.7 Confirm Host Name (Unix)

For Unix platforms, confirm that the host names are correctly formatted in the /etc/hosts file, and that this file contains entries for all hosts used by Oracle Fusion Applications to ensure that all hosts are visible from the primordial host. The /etc/hosts file is a network configuration file that associates IP addresses with host names and host alias names, if used. Every hosts file in Unix platforms should have an entry for the IP address 127.0.0.1, with the name localhost following it.

For more information, see "Edit Host Names (Linux)" in the *Oracle Fusion Applications Installation Guide*.

5.2.8 Add -d64 Option to JRE_MEMORY_OPTIONS (Solaris X64 and Solaris Sparc)

Add the -d64 option to JRE_MEMORY_OPTIONS in the following file:

APPLICATIONS_BASE/fusionapps/applications/oui/oraparam.ini

Adding this option prevents OPatch from failing with this error:

APPLICATIONS_BASE/fusionapps/applications/oui/lib/intelsolaris/liboraInstaller.so: wrong ELF class: ELFCLASS64 (Possible cause: architecture word width mismatch)

5.2.9 Confirm the Local Port Range Value

Check the local port range value in /proc/sys/net/ipv4/ip_local_port_ range before starting the installation. The recommended value is 32768 61000. If the range is set to any value below 32768, a system process could potentially use a port that was assigned to one of the Managed Servers. Since RUP Installer requires all domains to be down, those ports are available for the system to use.

To set the correct local port range, log in as the root user and run the following command:

```
echo "32768 61000" > /proc/sys/net/ipv4/ip_local_port_range
```

5.2.10 Confirm Database Settings

Perform the following steps to confirm that your database settings are optimized for the installation:

1. Refer to Oracle Fusion Applications release notes for information about database tuning parameters, to avoid time out conditions during the installation.

2. Confirm that the open file limit is set properly.

   RUP Installer uses multiple workers for uploading database content. The number of workers used dictates the open file limit setting for the machine where you run the RUP Installer. To understand how the number of workers are calculated and the requirement for the open file limit setting for the workers, see Section 3.1.2, "Patching Database Artifacts". For more information, see "Increase the Open Files Limit" in the *Oracle Fusion Applications Installation Guide*

3. Confirm that the SQL*Net Timeout Configuration is set properly.

   The exact setting in your environment depends on your network configuration and machine resources. Refer to "SQLNET.EXPIRE_TIME Parameter" and "INBOUND_CONNECT_TIMEOUT Parameter" in the *Oracle Fusion Applications Performance and Tuning Guide* to determine the parameters that need to be set.

5.2.11 Confirm All Oracle Homes Are Registered in the Central Inventory

Oracle Provisioning records information about the following Oracle homes separately from information about other products: Oracle Business Intelligence (Oracle BI), Oracle Global Order Promising (GOP), Web Tier, and Web Tier Common Oracle home installation information. RUP Installer expects information about all products to be recorded in the same place. To transfer information about the Oracle BI, GOP, and Web Tier installations to the same location as information about other products, perform the following steps. For more information about home directories, see "Provisioned Oracle Fusion Applications Home Directories" in the *Oracle Fusion Applications Administrator's Guide*.

1. Verify that the default Inventory Pointer file points to the central inventory on the primordial host on which RUP Installer runs. The default Inventory Pointer is in the following locations:

   - Unix: /etc/oraInst.loc

   - Solaris: `/var/opt/oracle/oraInst.loc`

   - Windows: located in the registry key, `\\HKEY_LOCAL_ MACHINE\\Software\Oracle\inst_loc`

2. Run `attachHome` from the BI Oracle home, for example, *APPLICATIONS_ BASE*/fusionapps/bi.

   ```
   (Unix) BI_HOME/oui/bin/attachHome.sh -jreLoc JAVA_HOME_LOCATION
   (Windows) BI_HOME\oui\bin\attachHome.cmd -jreLoc JAVA_HOME_LOCATION
   ```

3. Run `attachHome` from the GOP Oracle home, for example, *APPLICATIONS_ BASE*/fusionapps/gop.

   ```
   (Unix) GOP_HOME/oui/bin/attachHome.sh -jreLoc JAVA_HOME_LOCATION
   (Windows) GOP_HOME\oui\bin\attachHome.cmd -jreLoc JAVA_HOME_LOCATION
   ```

4. Run `attachHome` from the Web Tier Oracle home, for example, *APPLICATIONS_BASE*/webtier_mwhome/webtier.

```
(Unix) WEBTIER_HOME/oui/bin/attachHome.sh -jreLoc JAVA_HOME_LOCATION
(Windows) WEBTIER_HOME\oui\bin\attachHome.cmd -jreLoc JAVA_HOME_LOCATION
```

5. Run `attachHome` from the Web Tier Common Oracle home, for example, *APPLICATIONS_BASE*/webtier_mwhome/oracle_common.

```
(Unix) WEBTIER_COMMON_HOME/oui/bin/attachHome.sh -jreLoc JAVA_HOME_LOCATION
(Windows) WEBTIER_COMMON_HOME\oui\bin\attachHome.cmd -jreLoc JAVA_HOME_LOCATION
```

6. Run `attachHome` from the Oracle Common Oracle home.

```
(Unix) APPLICATIONS_BASE/fusionapps/oracle_common/oui/bin/attachHome.sh -jreLoc
JAVA_HOME_LOCATION
(Windows) APPLICATIONS_BASE\fusionapps\oracle_common\oui\bin\attachHome.cmd
-jreLoc JAVA_HOME_LOCATION
```

7. Register the dependency between the BI Oracle home and Oracle Common Oracle home.

   Run Oracle Universal Installer with the `-updateHomeDeps` option and pass a dependency list. The syntax for the dependency list is:

```
HOME_DEPENDENCY_LIST={ORACLE_HOME:DEPENDENT_ORACLE_HOME}
```

   Example for Business Intelligence:

```
(Unix) BI_HOME/oui/bin/runInstaller -updateHomeDeps "HOME_DEPENDENCY_LIST=
{APPLICATIONS_BASE/fusionapps/bi:APPLICATIONS_BASE/fusionapps/oracle_common}"
-jreLoc JAVA_HOME_LOCATION

(Windows) BI_HOME\oui\bin\setup.exe -updateHomeDeps "HOME_DEPENDENCY_LIST=
{APPLICATIONS_BASE\fusionapps\bi:APPLICATIONS_BASE\fusionapps\oracle_common}"
-jreLoc JAVA_HOME_LOCATION
```

8. Register the dependency between Web Tier Oracle home and Web Tier Common Oracle home.

```
(Unix) WEBTIER_HOME/oui/bin/runInstaller -updateHomeDeps "HOME_DEPENDENCY_LIST=
{APPLICATIONS_BASE/webtier_mwhome/webtier:APPLICATIONS_BASE/webtier_
mwhome/oracle_common}"
-jreLoc JAVA_HOME_LOCATION

(Windows) WEBTIER_HOME\oui\bin\setup.exe -updateHomeDeps "HOME_DEPENDENCY_LIST=
{APPLICATIONS_BASE\webtier_mwhome\webtier:APPLICATIONS_BASE\webtier_
mwhome\oracle_common}"
-jreLoc JAVA_HOME_LOCATION
```

9. Verify that the central inventory now contains the correct GOP, BI, and Web Tier information. Open the `inventory.xml` file from the `ContentsXML` subdirectory in your central inventory directory using a text editor. You can find your central inventory directory by looking in the default Oracle Inventory pointer file mentioned in Step 1. Verify that there are entries for GOP and for BI, and that the BI entry lists the Oracle Common dependency you specified in Step 6. Do the same for Web Tier information. Ensure that you do not modify `inventory.xml` in any way, as this may corrupt your system.

   Example entries in inventory.xml:

```
<HOME NAME="OH1109401105" LOC="APPLICATIONS_BASE/fusionapps/gop" TYPE="O"
```

```
IDX="11">
<HOME NAME="OH198367808" LOC="APPLICATIONS_BASE/fusionapps/bi" TYPE="O"
IDX="12">
    <DEPHOMELIST>
        <DEPHOME LOC="APPLICATIONS_BASE/fusionapps/oracle_common"/>
    </DEPHOMELIST>
</HOME>
<HOME NAME="OH987588708" LOC="APPLICATIONS_BASE/webtier_mwhome/webtier"
TYPE="O" IDX="13">
    <DEPHOMELIST>
        <DEPHOME LOC="APPLICATIONS_BASE/webtier_mwhome/oracle_common"/>
    </DEPHOMELIST>
</HOME>
<HOME NAME="OH1271096710" LOC="APPLICATIONS_BASE/webtier_mwhome/oracle_common"
TYPE="O" IDX="14">
    <REFHOMELIST>
        <REFHOME LOC="APPLICATIONS_BASE/webtier_mwhome/webtier"/>
    </REFHOMELIST>
</HOME>
```

Note: Rerunning the ATTACH_HOME command does not cause any issues.

5.2.12 Update Oracle Fusion Middleware Schema Credentials

Run the preRupSeeding.py script to perform updates to seed several Oracle Fusion Middleware schema credentials for the schema upgrade. This script updates the rup2-preupg-parameters.property properties file.

1. Unzip the script and properties file.

   The script and properties file are located in the companionCD.zip, located under REPOSITORY_LOCATION/installers/companionCD.zip. These two files must be unzipped to APPLICATIONS_ BASE/fusionapps/applications/admin/preupg, as shown in the following command.

   ```
   unzip -j companionCD.zip -d APPLICATIONS_
   BASE/fusionapps/applications/admin/preupg
   ```

2. Enable write permission on the rup2-preupg-parameters.property file.

   ```
   chmod u+w APPLICATIONS_
   BASE/fusionapps/applications/admin/preupg/rup2-preupg-parameters.properties
   ```

3. Ensure that the Administration Server on the Common Domain and a WLS server are running, and run the following command.

   ```
   APPLICATIONS_BASE/fusionapps/oracle_common/common/bin/wlst.sh APPLICATIONS_
   BASE/fusionapps/applications/admin/preupg/preRupSeeding.py
   ```

   This script connects to the Administration Server and prompts you for the following values. You can press **Enter** to accept default values. Note that you must accept the default values for the **Oracle Access Manager domain name** and **Oracle Access Manager authorization** parameters.

   - WLST credentials, including the user name, password and server URL for the CommonDomain Administration server.

- Oracle Fusion Applications database credentials, including the Oracle Database host name, port number, and sid or service. These values can be found in the DB_CONNECT_STRING row of *FA_ORACLE_HOME*/admin FUSION_env.properties.

- SYSDBA user name and password.

- Various schema credentials including:

  – CRM_FUSION_MDS_SOA Schema Owner

  – CRM_FUSION_SOAINFRA Schema Owner

  – FIN_FUSION_MDS_SOA Schema Owner

  – FIN_FUSION_SOAINFRA Schema Owner

  – FUSION_ACTIVITIES Schema Owner

  – FUSION_APM Schema Owner

  – FUSION_BIPLATFORM Schema Owner

  – FUSION_OCSERVER11G Schema Owner

  – FUSION_ORA_ESS Schema Owner

  – FUSION_WEBCENTER Schema Owner

  – HCM_FUSION_MDS_SOA Schema Owner

  – HCM_FUSION_SOAINFRA Schema Owner

  – OIC_FUSION_MDS_SOA Schema Owner

  – OIC_FUSION_SOAINFRA Schema Owner

  – PRC_FUSION_MDS_SOA Schema Owner

  – PRC_FUSION_SOAINFRA Schema Owner

  – PRJ_FUSION_MDS_SOA Schema Owner

  – PRJ_FUSION_SOAINFRA Schema Owner

  – SCM_FUSION_MDS_SOA Schema Owner

  – SCM_FUSION_SOAINFRA Schema Owner

  – SEARCHSYS Schema Owner

  – SETUP_FUSION_SOAINFRA Schema Owner

- Oracle Access Manager Administrator user name and password.

- Oracle Access Manager Resource Webgate Administrator user name and password.

- Oracle Access Manager Administration Server host name.

- Oracle Access Manager Administration Server port number.

- Oracle Access Manager administrator user name.

- Oracle Access Manager mode, valid values are open, simple, and cert. There is no default value. Your OAM administrator should know this value.

- Oracle Access Manager domain name, you must accept the default value of OraFusionApp.

- Oracle Access Manager primary server name, the default value is `oam_server1`.

- Oracle Access Manager version number, the default value is `11`.

- Oracle Access Manager authorization scheme, you must accept the default value of `FAAuthScheme`.

- Presence of a load balancer, valid values are true and false. The default value is false.

- Oracle HTTP Server host name.

5.2.13 Maintain Versions of Customized BI Publisher Reports

Ensure that you have your own versions of any customized BI Publisher reports. If a RUP includes an update to a catalog object that was delivered with an Oracle Fusion application, the patch will overwrite any customizations applied to the original report. For more information, see "Before You Begin Customizing Reports" in the *Oracle Fusion Applications Extensibility Guide*.

5.2.14 Confirm That JDeveloper Customizations Can Be Merged

If you performed JDeveloper customizations to a SOA composite and then you deployed the composite to the SOA runtime, you must perform manual steps to merge your customizations. To ensure that your customizations can be merged successfully, review the recommendations in "Merging Runtime Customizations from a Previously Deployed Revision into a New Revision" in the *Oracle Fusion Applications Extensibility Guide* before you start RUP Installer.

You will merge your customizations during the RUP Installation, after the **Online Verification** configuration task fails. For more information, see Section 5.5.18, "Merging SOA Composite JDeveloper Customizations While Installing a RUP".

5.2.15 Verify Credentials in Oracle Directory Services Manager (ODSM)

Verify that the following credentials are present in ODSM by performing the following steps:

1. Log in to Oracle Internet Directory using ODSM: `http://ldap_host:port`/odsm, for example, `http://IDM_HOST:7005/odsm`. (Note that you cannot do this using `jexplorer`.)

2. Connect to a directory. Use the OID-OID connection, for example, where the User name is `cn=orcladmin` and the Password is *password*.

3. Go to the **Data Browser** tab. Go to `cn=oracle` internet directory and within the `cn=oracle` internet directory, go to `cn=DirectoryAdminGroup`.

4. Verify that this user entry is present in the Members section:

   `cn=PolicyRWUser,cn=users,dc=us,dc=oracle,dc=com`

5. If the entry is not present, click the add [+] button in the Members section and add the entry. Then apply the changes.
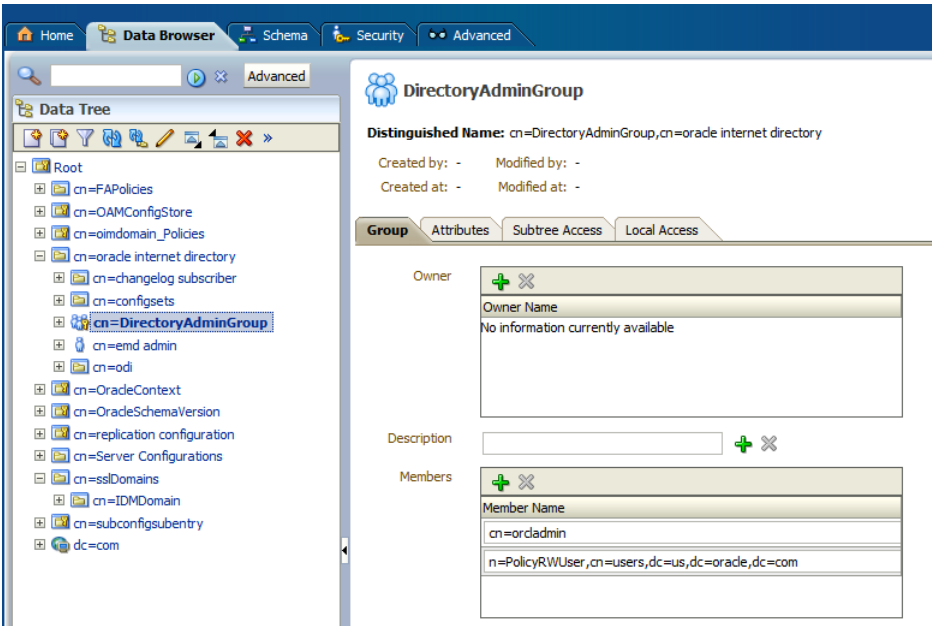
5.2.16 Verify the Default Realm Name is myrealm

RUP Installer expects the default realm name to be `myrealm` for the Common Domain. Verify that you have not changed this value to any other name, because changing the name to anything other than `myrealm` causes RUP Installer to fail. Log in to the WLS Console for the Common Domain and click **Security Realms** on the domain structure pane. A list of realms displays, where you can verify that there is an entry for `myrealm` and that it is the default realm.
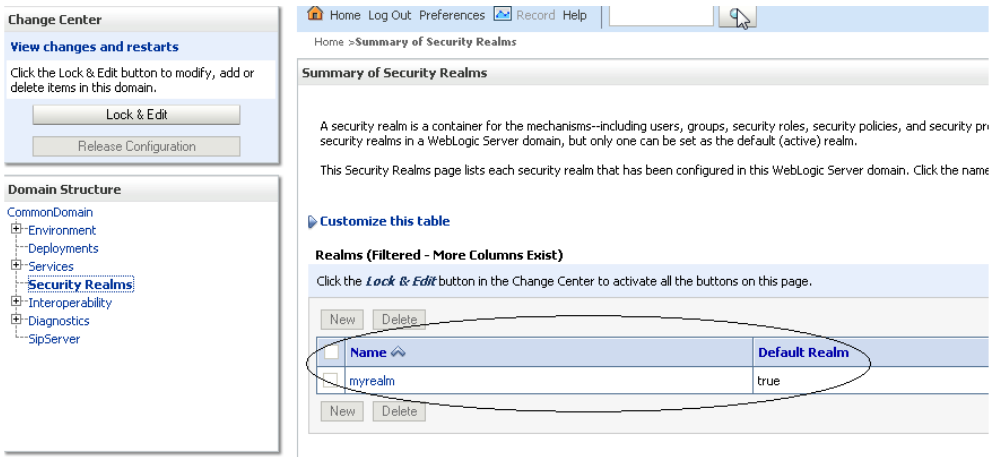
5.2.17 Save WebLogic Configuration Changes

RUP Installer makes WebLogic configuration changes using WebLogic Scripting Tool (WLST), which may overwrite any unsaved changes. Ensure that any pending WebLogic configuration changes are either activated or discarded. For more information, see "Configuring Existing WebLogic Domains" in *Oracle Fusion Middleware Oracle WebLogic Scripting Tool.*

5.3 Prepare to Install a RUP - During Downtime

This section describes the following preparation steps for installing a RUP, all of which must be performed during your system down time.

- Upgrade Identity Management Domain to the RUP2 Level
- Apply Mandatory Prerequisite Patches
- Verify the Status of Servers and Processes
- Perform Required Backups

5.3.1 Upgrade Identity Management Domain to the RUP2 Level

Perform the following steps to upgrade your Identity Management environment to the RUP2 level.

1. Stop all servers and processes in the Oracle Fusion Applications domain, except the OPSS Security Store and the database, before starting the Identity Management upgrade. If you want to use the fastartstop utility to do this, see "Starting and Stopping the Oracle Fusion Applications Middle Tier Using the fastartstop Utility" in the *Oracle Fusion Applications System Administrator's Guide*. Also confirm that the BI presentation servers are shut down.

2. Shut down the Oracle Enterprise Scheduler Service (ESS) server by performing the following steps:

    a. Stop the ESS request processor and dispatcher to prevent new requests from being processed. For more information, see "Starting and Stopping Oracle Enterprise Scheduler Service Components" in the *Oracle Fusion Applications Administrator's Guide*.

    b. Cancel any in-progress requests. For more information, see "Cancelling Oracle Enterprise Scheduling Server Job Requests" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Enterprise Scheduling Service*.

    c. Shutdown the ESS WebLogic Server Managed server. For more information, see the "Starting and Stopping" table, specifically the "Managed Server for an application" row, in the *Oracle Fusion Applications Administrator's Guide*.

3. Refer to Document ID 1435333.1 on My Oracle Support and follow the remaining mandatory Identity Management upgrade steps.

5.3.2 Apply Mandatory Prerequisite Patches

Perform the following steps to apply mandatory prerequisite patches before installing the RUP.

1. After you complete the Identity Management upgrade, confirm that all servers and processes in the Oracle Fusion Applications domain, except the OPSS Security Store and the database, are down before applying the prerequisite patches. If you want to use the fastartstop utility to do this, see "Starting and Stopping the Oracle Fusion Applications Middle Tier Using the fastartstop Utility" in the *Oracle Fusion Applications System Administrator's Guide*. Also confirm that the BI presentation servers are shut down. For Windows, see Section 5.3.2.1, "Stop Services on Windows Before Applying Mandatory Patches".

2. Apply mandatory Oracle Database patches mentioned in the "Oracle Database" section of Oracle Fusion Applications release notes.

3. Apply any additional prerequisite patches mentioned in the "Oracle Fusion Middleware" section of Oracle Fusion Applications release notes.

4. Apply all prerequisite patches mentioned in the "Applying Patches" section of Oracle Fusion Applications release notes.

5. If you have Oracle Business Intelligence Applications installed and configured, refer to Oracle Fusion Applications release notes for information about mandatory patches that need to be applied before installing the RUP. For additional information about patching Oracle Business Intelligence Applications, see "Oracle BI Applications Patching" in the *Oracle Fusion Middleware Reference Guide for Oracle Business Intelligence Applications*.

6. If additional ODI components, such as ODI SDK or ODI Studio are installed, you must run ODI Installer in UI mode to upgrade ODI to 11.1.1.6.0 before running RUP Installer. To determine if these additional ODI components are installed you can either use OPatch or you can look at the directories included under the ODI_HOME.

   To use OPatch, run `ODI_HOME\OPatch\opatch lsinventory` to get a list of installed products.

   Alternatively, you can look for the following directories under `ODI_HOME`:

   - `ODI_HOME\oracledi\client` will be present if ODI Studio was installed
   - `ODI_HOME\oracledi.sdk` will be present if ODI SDK was installed

   Note: You must follow the steps described in "Starting the Installer" and "Following the Installation Instructions for the 'Developer' Installations" in the *Oracle Fusion Middleware Installation Guide for Oracle Data Integrator*. You must install and upgrade your ODI Studio in an Oracle home other than Oracle Fusion Middleware Oracle homes and Oracle Fusion Applications Oracle home.

5.3.2.1 Stop Services on Windows Before Applying Mandatory Patches

For a Windows platform, the following services must be stopped:

- OracleOraDb11g_home1TNSListenerLISTENER_<SID>
- OracleOraDb11g_home1ClrAgent
- OracleDBConsole<SID>
- OracleJobScheduler<SID>
- OracleService<SID>
- OracleMTSRecoveryService
- Windows Management Instrumentation
- Distributed Transaction Coordinator
- Oracle <SID> VSS Writer Service

From the Control Panel, select **Administrative Tools**, then **Services**. Right click on each service and choose the **Stop** option.

5.3.3 Verify the Status of Servers and Processes

This section contains steps to follow for all platforms. For Windows platforms, also follow the steps in Section 5.3.3.10, "Steps for Windows Platforms".

To prevent locks on patched objects and other data issues during patching of database artifacts, review and perform the following checklist before installing the RUP.

5.3.3.1 Stop Running SES Schedules

Perform the following steps related to Oracle Secure Enterprise Search (SES).

1. Stop all running schedules.

    Get a list of running schedules by running the following command. The schedules with a status of EXECUTING are the running schedules.

    ```
    SES_ORACLE_HOME/bin/searchadmin -p ses_Admin_Password -c
    http://ses_Admin_Host:ses_Admin_Port/search/api/admin/AdminService
    getAllStates schedule
    ```

    Stop a running schedule by running the following command:

    ```
    SES_ORACLE_HOME/bin/searchadmin -p ses_Admin_Password -c
    http://ses_Admin_Host:ses_Admin_Port/search/api/admin/AdminService stop
    schedule -n schedule_Name
    ```

    > **Note:** To get a list of all schedules defined in Oracle SES, execute the following command:
    >
    > ```
    > SES_ORACLE_HOME/bin/searchadmin -p ses_Admin_Password -c
    >  http://ses_Admin_Host:ses_Admin_Port/search/api/admin/AdminService
    >  getAllObjectKeys schedule
    > ```

2. Deactivate the schedules that may start running during the RUP installation.

    The schedules that may start running during the RUP installation, such as daily schedules, must be deactivated. Execute the following command to deactivate such schedules:

    ```
    SES_ORACLE_HOME/bin/searchadmin -p ses_Admin_Password  -c
     http://ses_Admin_Host:ses_Admin_Port/search/api/admin/AdminService
     deactivate schedule -n schedule_Name
    ```

3. Stop the Index Optimizer.

    Run the following command to stop the Index Optimizer:

    ```
    SES_ORACLE_HOME/bin/searchadmin -p ses_Admin_Password -c
    http://ses_Admin_Host:ses_Admin_Port/search/api/admin/AdminService
    stop indexOptimizer
    ```

4. Deactivate the Index Optimizer if it may start running during the RUP installation.

    If the time at which the Index Optimizer is scheduled to run overlaps with the time period of the RUP installation, then the Index Optimizer must be deactivated before starting the RUP installation. Run the following command to deactivate the Index Optimizer:

    ```
    SES_ORACLE_HOME/bin/searchadmin -p ses_Admin_Password -c
    http://ses_Admin_Host:ses_Admin_Port/search/api/admin/AdminService
    ```

```
deactivate indexOptimizer
```

5.3.3.2 Stop the Node Manager and the OPMN Control Process

Stop the Node Manager and the OPMN control process. All OHS and Web Tier processes, including the Apache processes, must also be stopped if you are not running OHS from a separate installation (DMZ or otherwise). (On Windows, stop the Node Manager and OPMN services and follow steps 1 and 2 in Section 5.3.3.10, "Steps for Windows Platforms".) Note that you must start the Node Manager for all domains and the OPMN control process during the **Verifying Node Manager and OPMN Status** configuration task, before proceeding to the next step in the RUP installation.

For more information, see "Stopping Node Manager" in *Oracle Fusion Middleware Node Manager Administrator's Guide for Oracle WebLogic Server*.

Use the following procedure to stop the OPMN control processes for Oracle Business Intelligence, GOP, and Web Tier (OHS). This procedure also stops all BI server processes, all GOP processes, and the OHS process.

> **Note:** There should be no Web Tier processes on this installation if you are running OHS from a separate installation (DMZ or otherwise). In this case, you do not need to stop the Web Tier processes.

1. Set *ORACLE_INSTANCE* to the location of the target Oracle instance directory.

2. Go to the `bin` directory under the target Oracle instance directory.

3. Run the `opmnctl` program from the current directory with the `stopall` command.

The following example is for Oracle Business Intelligence, where *BIInstance* is the location of `BIInstance`. Depending on whether L**ocal Applications Config** is enabled for your setup, `BIInstance` is located under either the **Applications Config** directory or the **Local Applications Config** directory of the BI host.

```
(Unix)INSTANCE_HOME=APPLICATIONS_CONFIG/BIInstance; export INSTANCE_HOME
cd $ORACLE_INSTANCE/bin
./opmnctl stopall

(Windows) set INSTANCE_HOME=APPLICATIONS_CONFIG\BIInstance
cd $ORACLE_INSTANCE\bin
.\opmnctl stopall
```

Example for GOP:

```
(Unix)ORACLE_INSTANCE=APPLICATIONS_CONFIG/gop_1; export ORACLE_INSTANCE
cd $ORACLE_INSTANCE/bin
./opmnctl stopall

(Windows) set INSTANCE_HOME=APPLICATIONS_CONFIG\gop_1
cd $ORACLE_INSTANCE\bin
.\opmnctl stopall
```

Example for Web Tier (OHS):

```
(Unix) INSTANCE_HOME=APPLICATIONS_CONFIG/CommonDomain_webtier; export INSTANCE_
HOME
cd $ORACLE_INSTANCE/bin
./opmnctl stopall
```

```
(Windows) set INSTANCE_HOME=APPLICATIONS_CONFIG\CommonDomain_webtier
cd $ORACLE_INSTANCE\bin
.\opmnctl stopall
```

For more information about the location of *APPLICATIONS_CONFIG*, see Section 5.2.1, "Before You Begin".

For more information about concepts related to ORACLE_HOME and ORACLE_INSTANCE, refer to the "Understanding Oracle Fusion Middleware Concepts" chapter in the *Fusion Middleware Administrator's Guide*.

5.3.3.3 Start the OPSS Security Store

Start the OPSS Security Store if it is not already running. The OPSS Security Store used here is an Oracle Internet Directory LDAP server instance. Before proceeding with the RUP installation, the designated Oracle Internet Directory server instance must be up and running. If this server is not running prior to starting the installation, the related configuration tasks will fail. For more information, see Section 5.5.11, "LdapServerCheck Failure".

For more information about starting, see "Starting and Stopping Oracle Internet Directory" in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management (Oracle Fusion Applications Edition)*.

5.3.3.4 Confirm the First Node is Running in a RAC Database

If you are running on a RAC database, ensure that the first node (host and port) in the TNS descriptor is up and running prior to running RUP Installer. If this is not running, the Upgrading Middleware Schemas configuration task will fail.

5.3.3.5 Start Servers That Were Added After Provisioning

If you added any servers, you must start the new servers at least once before you run RUP Installer. This step is not required for a server that has previously been started at least once since you initially installed Oracle Fusion Applications.

5.3.3.6 Confirm the Database is Running and in Idle State

Confirm there are no active jobs or processes running against the database. If you stop all servers, including ESS servers, most Oracle Fusion Applications processes are shut down. However, some database jobs could still be running or scheduled to start. These processes must be stopped so that they do not start while patching is in progress. Stop all background jobs, including jobs in the database and active processes.

To confirm if the database is running in idle mode, you can follow the steps below:

1. Start SQL*Plus and connect as the SYS user and run the following SQL*Plus queries.

2. To retrieve a list of active SQL processes:

    ```
    select a.sid, a.serial#, b.sql_text
    from v$session a, v$sqlarea b
    where a.sql_address=b.address
    and a.username in ('FUSION', 'FUSION_RUNTIME')
    and a.sid <> sys_context('USERENV', 'SID');
    ```

3. To retrieve a list of scheduler jobs that are currently running:

    ```
    select owner, job_name
    from dba_scheduler_running_jobs;
    ```

4. To retrieve a list of scheduled jobs for the next 24 hours:

```
select owner, job_name from dba_scheduler_jobs
where state = 'SCHEDULED' and next_run_date
between sysdate and sysdate+1;
```

If all the queries return no rows, that indicates the database is in Idle mode for the next 24 hours and you can safely proceed with the upgrade.

5.3.3.7 Confirm All Oracle Fusion Applications Patch Manager Processes Are Complete

From your operating system, check for processes that are running `fapmgr`, `javaworker`, `adpatch`, `adadmin`, and `adworker`. If an `fapmgr` session was interrupted, you may need to `forcefail` and abandon the session as follows:

1. Use the `fapmgr forcefail` command to update the patching tables.

   (UNIX) *FA_ORACLE_HOME*/lcm/ad/bin/fapmgr.sh forcefail [-logfile *log file name*] [-loglevel *level*]

   (Windows) *FA_ORACLE_HOME*\lcm\ad\bin\fapmgr.cmd forcefail [-logfile *log file name*] [-loglevel *level]*

   If the forcefail command returns "There are no active Oracle Fusion Applications Patch Manager sessions which can be forcibly failed", then skip the next step.

2. Use the `fapmgr abort` command to abandon the session, only if a session is active.

   (UNIX) *FA_ORACLE_HOME*/lcm/ad/bin/fapmgr.sh abort [-logfile *log file name*] [-loglevel *level*]

   (Windows) *FA_ORACLE_HOME*/lcm\ad\bin\fapmgr.cmd abort [-logfile *log file name*] [-loglevel *level*]

5.3.3.8 Confirm All Oracle Fusion Applications AutoPatch Processes are Complete

If an Oracle Fusion Applications AutoPatch session is running, you must abandon the session as follows.

Run the following command from *ATGPF_ORACLE_HOME:* (This is the directory under *MW_HOME* that contains the Applications Core code. For more information, see Section 7.1.2, "Running Oracle Fusion Applications AutoPatch".)

(Unix) lcm/ad/bin/adpatch.sh abandon=y interactive=n defaultsfile=*ATGPF_ORACLE_HOME*/admin/*TWO_TASK*/*defaults*.txt logfile=*logfile_name*.log

(Windows) lcm\ad\bin\adpatch.cmd abandon=y interactive=n defaultsfile=*ATGPF_ORACLE_HOME*\admin*LOCAL**defaults*.txt logfile=*logfile_name*.log

The *TWO_TASK* value can be obtained from the `ATGPF_env.properties` file.

The *LOCAL* value can be obtained from the `FUSION_env.properties` file.

5.3.3.9 Confirm All AD Administration Sessions Are Complete

If an AD Administration session is running, you must abandon the session as follows:

1. From *FA_ORACLE_HOME:*

   (Unix) lcm/ad/bin/adadmin.sh abandon=y interactive=n defaultsfile=*FA_ORACLE_*

HOME/admin/*TWO_TASK*/*defaults*.txt logfile=*log_file_name*

(Windows) lcm\ad\bin\adadmin.cmd abandon=y interactive=n defaultsfile=*FA_ ORACLE_HOME*\admin*LOCAL*\defaults.txt logfile=*log_file_name*

The *TWO_TASK* and *LOCAL* values can be obtained from the FUSION_ env.properties file.

2. From *ATGPF_ORACLE_HOME*

(Unix) lcm/ad/bin/adadmin.sh abandon=y interactive=n defaultsfile=*ATGPF_ORACLE_ HOME*/admin/*TWO_TASK*/*defaults*.txt logfile=*log_file_name*

(Windows) lcm\ad\bin\adadmin.cmd abandon=y interactive=n defaultsfile=*ATGPF_ ORACLE_HOME*\admin*LOCAL*\defaults.txt logfile=*log_file_name*

The *TWO_TASK* and *LOCAL* values can be obtained from the ATGPF_ env.properties file.

5.3.3.10 Steps for Windows Platforms

Follow these steps before you install a RUP on a Windows platform.

1. Change the service type from Automatic to Manual for the following services: Node Manager, Web Tier, GOP, and BI. Restore the service type back to Automatic after RUP installation completes.

2. Stop the following services: Node Manager, Web Tier, GOP, and BI.

3. Reboot the Oracle Fusion Applications host.

4. Release Java Archive File Handles on System Process ID (PID) 4

   On the Windows WebLogic Server, the Node Manager runs as a service. Since, the *APPLICATIONS_BASE* of Oracle Fusion Applications is in a symbolic folder, some of the jar file handles are loaded by Microsoft Windows System Process ID (PID) 4. The loaded file handles eventually cause Middleware patch application to fail when running the RUP Installer. Before starting the RUP Installer, make sure the Windows System Process ID (PID) 4 does not have handles to Oracle Fusion Applications jar files.

   Check for file handles using the Windows utility Process Explorer. If file handles exist, make sure the Node Manager service is not running. If the file handles remain even after shutting down the Node Manager service, switch the Node Manager service from Automatic to Manual and reboot the machine to release the file handles.

5. Ensure that the Server service is up and running.

6. Increase the shared_pool_size in the init.ora file. If it seems large enough then improve segmentation in the shared pool by reserving part of the shared pool for large objects using the SHARED_POOL_RESERVED_SIZE parameter. The recommended value to start tuning is one third of the shared pool size. You can allow for large objects by using the SHARED_POOL_RESERVED_MIN_ALLOC parameter.

5.3.4 Perform Required Backups

The following backups must be performed before you install a RUP:

- Back Up Oracle Fusion Applications
- Back Up the OPSS Security Store

- [Back Up Applications and System Policies](#)

- [Back Up Oracle Business Intelligence RPD Customizations](#)

- [Back Up Steps for Windows Platforms](#)

5.3.4.1 Back Up Oracle Fusion Applications

Back up your entire Oracle Fusion Applications environment by following the steps in "Backing Up and Recovering Oracle Fusion Applications" in the *Oracle Fusion Applications Administrator's Guide*. For additional back up steps that are specific to Windows, refer to Section 5.3.4.5, "Back Up Steps for Windows Platforms". You should also back up your central inventory.

5.3.4.2 Back Up the OPSS Security Store

RUP Installer upgrades all WLS domains to the 11gR1 PS5 MLR1 (11.1.1.6.1) level so you must perform the following backups. Make sure you perform your backups in directories that you can restore from. You can use any directory to back up the data, as long as you know where to restore the backup from.

1. **OPSS Security Store**

   Back up all data under the root node of the OPSS Security Store. To identify the root node in the Oracle Internet Directory hosting the OPSS Security store, use Fusion Applications Control and look at the Root Node Details pane under the Security Provider information. For more information, see "Reassociating with Fusion Middleware Control" in the *Oracle Fusion Middleware Application Security Guide*.
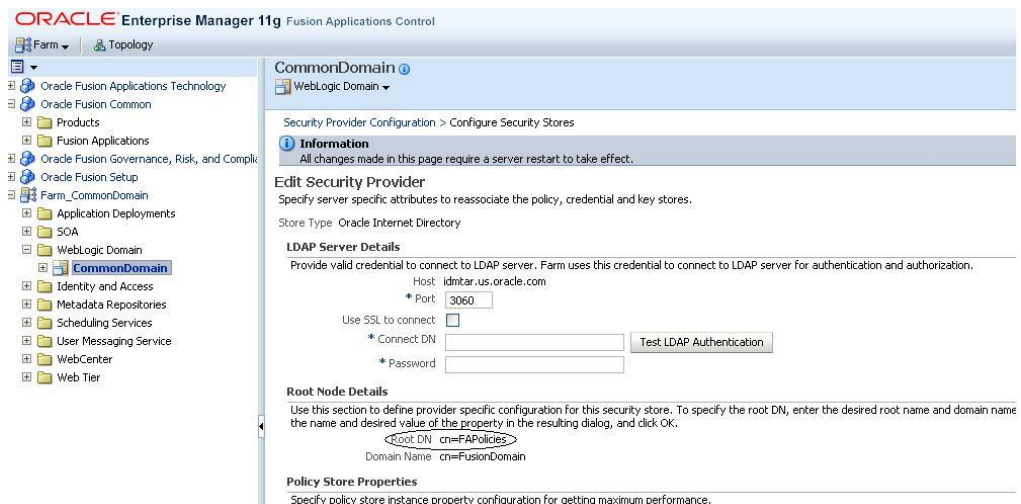
   In case of an upgrade failure, restore this node entirely. The `ldifwrite` and `bulkload` operations that follow must be performed on the system where the Oracle Internet Directory hosting the OPSS Security store resides.

   - Set the following environment variables.

     ```
     setenv ORACLE_HOME   OID_ORACLE_HOME
     setenv ORACLE_INSTANCE   OID_INSTANCE_HOME
     ```

     Example:

     ```
     setenv ORACLE_HOME /u01/oid/oid_home
     setenv ORACLE_INSTANCE /u01/oid/oid_inst
     ```

- Follow this step to create the backup.

  In the system where the Oracle Internet Directory is located, produce an LDIF file by running `ldifwrite` as illustrated in the following line:

  ```
  OID_HOME/ldap/bin/ldifwrite connect="srcOidDbConnectStr"
  basedn="cn=FAPolicies", c=us" ldiffile="srcOid.ldif"
  ```

  Example:

  ```
  /u01/oid/oid_home/ldif/bin/ldifwrite connect="oidddb"
  basedn="cn=FAPolicies" ldiffile="srcOid.ldif"
  ```

  This command writes all entries under the node `cn=FAPolicies` to the file `srcOid.ldif`. Once generated, move this file to the directory that was identified earlier, to hold all backup data.

- Follow these steps to restore the backup.

  - In the Oracle Internet Directory system, verify that there are no schema errors or bad entries by running `bulkload` as illustrated in the following line:

    ```
    OID_HOME/ldap/bin/bulkload connect="dstOidDbConnectStr" check=true
    generate=true restore=true file="fullPath2SrcOidLdif"
    ```

    If duplicate DNs (common entries between the source and destination directories) are detected, review them to prevent unexpected results.

  - Load data into the Oracle Internet Directory by running `bulkload` as illustrated in the following line:

    ```
    OID_HOME/ldap/bin/bulkload connect="dstOidDbConnectStr" load=true
    file="fullPath2SrcOidLdif"
    ```

For more information about the `bulkload` command, see "Performing Bulk Operations" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

For more information about migrating Oracle Internet Directory, see "Migrating Large Volume Policy and Credential Stores" in th*e Oracle Fusion Middleware Application Security Guide*.

2. **Bootstrap Wallet**

   Back up the `cwallet.sso file` in the *DOMAIN_HOME*`/config/fmwconfig/bootstrap` directory for **each WLS domain** in an Oracle Fusion Applications installation. You must take backups of each `cwallet.sso` file for each domain and when you restore, you must be careful to restore the correct file. For example, if you back up `cwallet.sso` from the Common Domain, then you must restore it in the Common Domain upon failure. If you back up `cwallet.sso` from the BI domain, you must restore it in the BI Domain upon failure.

5.3.4.3 Back Up Applications and System Policies

Back up applications and system policies for each stripe supported by Oracle Fusion Applications. System policies are global and not by stripe. Applications policies are stored by stripe and must be backed up and restored by stripe. If you do not back up the policies by stripe, you cannot restore the policies from your backup. Oracle Fusion Applications supports the following stripes:

- `fscm_system-jazn-data.xml`: FSCM stripe

- `crm_system-jazn-data.xml`: CRM stripe

- `hcm_system-jazn-data.xml`: HCM stripe

- `bip_jazn-data.xml`: OBI stripe

The following steps explain how to back up the system policies and the four application stripes from an Oracle Internet Directory (OID) OPSS security store to individual XML files. These steps must be performed on the Common Domain.

1. Copy the existing `jps-config-jse.xml` file (that has configured the `policystore.ldap` service) to a new file, `myFile-migrate-jps-config.xml`. This is the `jps-config-jse.xml` file that is referenced in the `FUSION_env.properties` file.

2. Open `myFile-migrate-jps-config.xml` for editing and add the following `jpsContexts`:

   ```
   <jpsContext name="MyOIDSecurityStore">
     <serviceInstanceRef ref="policystore.ldap"/>
   </jpsContext>

   <jpsContext name="MyDestinationContextFscm">
     <serviceInstanceRef ref="my.fscm.backup"/>
   </jpsContext>

   <jpsContext name="MyDestinationContextCrm">
     <serviceInstanceRef ref="my.crm.backup"/>
   </jpsContext>

   <jpsContext name="MyDestinationContextHcm">
     <serviceInstanceRef ref="my.hcm.backup"/>
   </jpsContext>

   <jpsContext name="MyDestinationContextObi">
     <serviceInstanceRef ref="my.obi.backup"/>
   </jpsContext>

   <jpsContext name="MyDestinationContextGlobal">
     <serviceInstanceRef ref="my.global.backup"/>
   </jpsContext>
   ```

3. Add the following service instances to `myFile-migrate-jps-config.xml`. You must create a `backup_directory` to hold the exported policy XML files before following this step.

   ```
   <serviceInstance location="backup_directory/fscm-policies.xml"
    name="my.fscm.backup" provider="policystore.xml.provider">
   <property name="createNew" value="true"/> </serviceInstance>

   <serviceInstance location="backup_directory/crm-policies.xml"
    name="my.crm.backup" provider="policystore.xml.provider">
   <property name="createNew" value="true"/> </serviceInstance>

   <serviceInstance location="backup_directory/hcm-policies.xml"
    name="my.hcm.backup" provider="policystore.xml.provider">
   <property name="createNew" value="true"/> </serviceInstance>

   <serviceInstance location="backup_directory/obi-policies.xml"
    name="my.obi.backup" provider="policystore.xml.provider">
   ```

```
<property name="createNew" value="true"/> </serviceInstance>

<serviceInstance location="backup_directory/global-policies.xml"
 name="my.global.backup" provider="policystore.xml.provider">
<property name="createNew" value="true"/> </serviceInstance>
```

4. Remove or comment out the entry `<serviceInstanceRef ref="idstore.ldap"/>` which exists in `<jpsContext name="default">...</jpsContext>`.

5. Create five XML files, `fscm-policies.xml`, `crm-policies.xml`, `hcm-policies.xml`, `obi-policies.xml` (one for each application stripe), and `global-policies.xml` (for system policies), each containing the following framework:

```
<?xml version="1.0" encoding='utf-8' ?>
  <jazn-data>
    <jazn-realm default="jazn.com">
      <realm>
            <name>jazn.com</name>
      </realm>
    </jazn-realm>
  <policy-store>
    <applications>
    </applications>
  </policy-store>
  <jazn-policy>
  </jazn-policy>
  </jazn-data>
```

6. Use the migrateSecurityStore OPSS WLST command to backup each application stripe:

```
migrateSecurityStore(type="appPolicies",
configFile="jpsConfigFileLocation", src="MyOIDSecurityStore",
dst="dstJpsContext", srcApp="srcAppName")
```

Where:

jpsConfigFileLocation is the location of the file, `myFile-migrate-jps-config.xml`.

srcAppName is the stripe being backed up, such as `fscm`.

dstJpsContext is the name of the context that refers to the XML store, such as, `MyDestinationContextFscm`.

7. Use the OPSS WLST command `migrateSecurityStore` to backup system policies. Run the following command from *ORACLE_COMMON_HOME*, which is defined in the `FUSION_env.properties` file:

```
ORACLE_COMMON_HOME/common/bin/wlst.sh

migrateSecurityStore(type="globalPolicies",
configFile="jpsConfigFileLocation", src="srcJpsContext",
dst="dstJpsContext")
```

Where:

`jpsConfigFileLocation` is the location of the file `myFile-migrate-jps-config.xml`.

srcJpsContext is the name of the context that refers to the OID security store, such as, *MySourceContext*.

dstJpsContext is the name of the context that refers to the XML policy store, such as *MyDestinationContextGlobal*.

For more information, see "Migrating with the Script migrateSecurityStore" in the *Oracle Fusion Middleware Application Security Guide*.

5.3.4.4 Back Up Oracle Business Intelligence RPD Customizations

If you made customizations to the content of the Oracle Business Intelligence Repository (Oracle BI RPD), perform the following steps:

1. Ensure that you have a backup of the original version of the Oracle Fusion Applications 11g Oracle BI RPD. If you do not have a backup created before making customizations, then use a version of the RPD in the following instance directory after provisioning:

```
APPLICATIONS_
BASE/instance/BIInstance/bifoundation/OracleBIServerComponent/coreapplication_
obis1/repository/OracleBIApps_BI0002.rpd
```

2. Back up your existing customized version of the Oracle Fusion Applications 11g Oracle BI RPD by copying the file from your runtime location to a safe place of your choosing for later use. To find out what the current, custom Oracle BI RPD file is called, use Oracle Fusion Middleware Control and locate the file in the following directory:

```
APPLICATIONS_
BASE/instance/BIInstance/bifoundation/OracleBIServerComponent/coreapplication_
obis1/repository/
```

For information about how to resolve conflicts related to your customizations after RUP installation, see Section 5.5.20, "Failure During Applying BI Metadata Updates".

5.3.4.5 Back Up Steps for Windows Platforms

Back up the Oracle Fusion Applications environment, including *APPLICATIONS_BASE*, inventory, registry entries, Oracle Identity Management, the database and the System environment PATH variable of the Oracle Fusion Applications host machine.

1. *APPLICATIONS_BASE* has many files whose path is more than 256 characters. The Microsoft Windows Copy function is limited to copying only those files with a path of less than 256 characters. Therefore, many files fail to copy.

Use Robust File Copy (Robocopy), which is available as part of the Windows Resource Kit, to copy the *APPLICATIONS_BASE*. Use the following command:

```
robocopy <source> <destination> /MIR > <file>
```

Sample output from the robocopy command:

	Total	Copied	Skipped	Mismatch	FAILED	Extras
Dirs:	112640	112640	0	0	0	
Files:	787114	787114	0	0	0	
Bytes:	63.822 g	63.822 g	0	0	0	
Times:	2:22:20	2:19:00			0:00:00	0:03:19

2. Back up the inventory.

   Back up the inventory location referenced in the registry `HKEY_LOCAL_`
   `MACHINE\SOFTWARE\ORACLE\inst_loc`.

3. Back up the registry.

   Use `Regedit.exe` to back up the following registries related to Oracle Fusion
   Applications.

   ■ HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

      – Web Tier service

      – BI Service

      – Node Manager service

   ■ HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE

   ■ HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Oblix

4. Ensure that the System PATH has the following values:

```
C:\<APPLICATIONS_BASE>\dbclient\bin
C:\<APPLICATIONS_BASE>\webtier_mwhome\webtier\bin
C:\<APPLICATIONS_BASE>\webtier_mwhome\webtier\opmn\bin
C:\<APPLICATIONS_BASE>\webtier_mwhome\webtier\opmn\lib
C:\<APPLICATIONS_BASE>\webtier_mwhome\webtier\perl\bin
C:\<APPLICATIONS_BASE>\fusionapps\bi\products\Essbase\EssbaseServer\bin
C:\<APPLICATIONS_BASE>\fusionapps\bi\bin
C:\<APPLICATIONS_BASE>\fusionapps\bi\opmn\bin
C:\<APPLICATIONS_BASE>\fusionapps\bi\opmn\lib
C:\<APPLICATIONS_BASE>\fusionapps\bi\perl\bin
```

   Add any of the previous values that are missing to the system PATH. Missing
   values cause failures in launching the Oracle Process Manager and Notification
   Server (OPMN) services and Oracle Business Intelligence Presentation Services
   Web Catalog (Webcat) deployment tasks in RUP Installer.

5. Save the system PATH variable.

5.4 Install a RUP

RUP Installer must run during down time. Oracle recommends that you run RUP
Installer from a machine that is co-located in the same subnetwork as the database
server to maximize performance. You must run RUP Installer from the primordial
host.

This section contains the steps to install a RUP with RUP Installer. It contains the
following topics:

■ Perform the Installation

■ Complete the Post Installation Tasks

5.4.1 Perform the Installation

Ensure that the steps in Section 5.2, "Prepare to Install a RUP - Pre-Down Time" and
Section 5.3, "Prepare to Install a RUP - During Downtime" are successfully completed
before installing the RUP.

> **Note:** If you encounter errors during the RUP installation, refer to
> Section 5.5, "Troubleshoot RUP Installer Sessions" before clicking any
> buttons in the RUP Installer User Interface.

5.4.1.1 Start RUP Installer

Start RUP Installer from the command line, using specific options to further define the
necessary actions. You must run RUP Installer from the primordial host.

1. Set the *JAVA_HOME* environment variable as follows:

   ```
   (Unix) export JAVA_HOME=APPLICATIONS_BASE/fusionapps/jdk6

   (Windows) set JAVA_HOME=APPLICATIONS_BASE\fusionapps\jdk6
   ```

2. Confirm the registration of the network location of *FA_ORACLE_HOME*.

   If the Oracle Fusion Applications Oracle home directory (*FA_ORACLE_HOME*),
   which is *APPLICATIONS_BASE*/fusionapps/applications, is registered in
   the central inventory with a /net path, then provide the oraInst.loc location
   including /net when starting RUP Installer. An example follows:

   ```
   REPOSITORY_LOCATION/installers/farup/Disk1/runInstaller -jreLoc APPLICATIONS_
   BASE/fusionapps/jdk6/ -invPtrLoc /net/APPLICATIONS_
   BASE/fusionapps/applications/oraInst.loc
   ```

   If not triggered with /net path, RUP Installer copies the -invPtrLoc file to *FA_
   ORACLE_HOME*. In the example, this results in a copy of the file to itself, which
   results in a zero byte file. This causes failure during the copy phase when
   oracle_common patches are applied. For more information, see Section 5.5.2.3,
   "Inventory Pointer File is Empty".

3. Start RUP Installer.

   ```
   (UNIX) REPOSITORY_LOCATION/installers/fusionapps/Disk1/runInstaller -jreLoc
   JAVA_HOME_LOCATION [-invPtrLoc FA_ORACLE_HOME/oraInst.loc] \
   [-J-Dworkers=number_of_workers][-J-DlogLevel=level]
   [logfile=log_file_name][-debug yes]

   (IBM AIX on POWER Systems (64-bit)
   REPOSITORY_LOCATION/installers/farup/Disk1/runInstaller -jreLoc
   JAVA_HOME_LOCATION [-invPtrLoc FA_ORACLE_HOME/oraInst.loc] \
   [-J-Dworkers=number_of_workers][-J-DlogLevel=level]
   [-J-DserverStartTimeout=timeout_period_for_server_in_seconds]
   [logfile=log_file_name][-debug yes]
   JVM_OPTIONS="-Xms1024m -Xmx1536m"

   (Solaris X64 and Solaris Sparc)
   REPOSITORY_LOCATION/installers/fusionapps/Disk1/runInstaller -jreLoc
   JAVA_HOME_LOCATION [-invPtrLoc FA_ORACLE_HOME/oraInst.loc] \
   [-J-Dworkers=number_of_workers][-J-DlogLevel=level]
   [logfile=log_file_name][-debug yes]
   JVM_OPTIONS="-d64 -Xmx1024m -XX:MaxPermSize=1024m"

   (Windows)REPOSITORY_LOCATION\installers\fusionapps\Disk1\setup.exe -jreLoc
   JAVA_HOME_LOCATION [-Dworkers=number_of_workers][-DlogLevel=level]
   [logfile=log_file_name] [-debug yes]
   ```

   Table 5–3 shows valid options that can be used when running RUP Installer.

Table 5–3   RUP Installer command options

Argument	Description	Mandatory
-jreLoc	Path where the Java Runtime Environment is installed. This option does not support relative paths, so you must specify the absolute path.	Yes.
-invPtrLoc	The location of an overriding inventory pointer file. If Oracle Fusion Applications Oracle home directory (*FA_ORACLE_HOME*), located under the APPLICATIONS_ BASE/fusionapps directory, is registered in inventory with a /net path, then provide the oraInst.loc including /net in the path.	Recommended, use to override the default location of the inventory pointer file, located in /etc/oraInst.loc. This option can be used only on Unix platforms.
-J-Dworkers (-Dworkers for Windows)	The number of workers to use for uploading database content. If you provide a value for the number of workers that is outside the calculated range, you are prompted to provide a value that is within the optimal range. If you do not use this option, a calculated optimal value is used.	No, overrides the default number of workers calculated by RUP Installer. See "Worker Calculation" in Section 3.1.2, "Patching Database Artifacts".
-J-DlogLevel (-DlogLevel for Windows)	Records messages in the log file at the level you specify. Enter a value to override the default log level of INFO. See Section 11.1, "Oracle Fusion Applications Patch Manager Logging".	No, default value is INFO.
-debug	Retrieves the debug information from RUP Installer.	No.

Example:

```
(Unix) REPOSITORY_LOCATION/installers/fusionapps/Disk1/runInstaller -jreLoc
 APPLICATIONS_BASE/fusionapps/jdk6 -invPtrLoc FA_ORACLE_HOME/oraInst.loc

(Windows) REPOSITORY_LOCATION\installers\fusionapps\Disk1\setup.exe
-jreLoc APPLICATIONS_BASE\fusionapps\jdk6
```

Example when *FA_ORACLE_HOME* is registered with a /net path:

```
REPOSITORY_LOCATION/installers/fusionapps/Disk1/runInstaller -jreLoc
APPLICATIONS_BASE/fusionapps/jdk6 -invPtrLoc /net/FA_ORACLE_HOME/oraInst.loc
```

5.4.1.2 Run RUP Installer

Table 5–4 illustrates the tasks that RUP installer runs. For information about troubleshooting RUP Installer sessions, see Section 5.5, "Troubleshoot RUP Installer Sessions". For information about log files generated during RUP installation, see Section 5.5.1, "RUP Installer Log File Directories".

Table 5–4   RUP Installer Screen Sequence

Screen	Description and Action Required
Welcome	Appears when you start RUP Installer. This screen does not appear if you restart RUP Installer after a failure. The standard Welcome screen is read-only. It contains a navigation pane on the left-hand side that summarizes the tasks the installer will take. Each item in the pane represents an installer screen, which contains prompts for the necessary information. Click **Next** to continue.
Installation Location	Specify the location of the existing Oracle Fusion Applications home (*FA_ORACLE_HOME)* where you want to install the RUP. Click **Next** to continue.
Installation Summary	Summarizes the selections you made during this installation session. It includes the Oracle home, required and available disk space, and the version of the RUP to be installed. Review the information displayed to ensure that the installation details are what you intend. To make changes before installing, click **Back** to return to previous screens in the interview. Click **Install** to accept this configuration and start the installation.
Installation Progress	Displays a progress indicator that shows the percentage of the installation that is complete and indicates the location of the installation log file. The installation task consists of copying files from the RUP to the appropriate Oracle homes. The configuration process starts when the installation progress indicator shows 100 percent. Click **Next** to continue.

Table 5–4 (Cont.) RUP Installer Screen Sequence

Screen	Description and Action Required
Policy Store Analysis (Note that if you installed a Language Pack and chose to override the base English strings in the policy store, then this screen no longer displays during RUP installation.)	Analysis is available for the following policy store stripes: hcm, crm, fscm, and obi. Select the stripes to be analyzed and then click **Run Analysis** to identify any conflicts or deletions. Only the stripes that will be updated are enabled for analysis and the analysis could run for several minutes. After the analysis runs, review the results of the analysis to determine which deployment method RUP Installer will use for policy store changes to each stripe. Oracle recommends that you select **Apply safe changes only**. This is the safest method unless you have read and totally understood the consequences of the other three options. If you decide to resolve the conflicts or deletions before the actual JAZN upload from RUP Installer, you should run the Policy Store Analysis step again to get the most accurate analysis report. The choices for deployment method are: ■ Apply safe changes only (choose this method if there are no conflicts) ■ Apply all changes and overwrite customizations ■ Append additive changes ■ Manually resolve conflicts and upload changes using Authorization Policy Manager If you choose **Apply safe changes only** or **Append additive changes**, then you must review the results of the analysis to manually upload any changes not applied by RUP Installer with the choice you selected, after the installation is complete. If you choose **Apply all changes and overwrite customizations**, then you may need to reapply the customizations that are overwritten after the installation is complete. If you choose one of these options, click **Next** after you make your selection. If you choose **Manually resolve conflicts and upload changes using Authorization Policy Manager** (APM), you must pause the upgrade while you bring up the APM application and upload the changes. For more information, see the "Upgrading Oracle Fusion Applications Policies" chapter in the *Oracle Fusion Middleware Oracle Authorization Policy Manager Administrator's Guide (Oracle Fusion Applications Edition)*. Note the location of the following files: ■ Baseline file: `FA_ORACLE_HOME`/admin/JAZN/`stripe`/baseline ■ Patch file for fscm, crm, and hcm stripes: `FA_ORACLE_HOME/stripe`/deploy/system-jazn-data.xml ■ Patch file for the obi stripe: `FA_ORACLE_HOME`/com/acr/security/jazn/bip_jazn-data.xml When you complete this task in APM, shut down the APM application, return to RUP Installer, and click **Next**.
Configuration Progress	Displays a progress indicator that shows the percentage of the configuration phase that is complete. It displays each task, including steps within tasks, in the message pane as it is performed. Tasks that could be included in the configuration phase are described in Section 5.1.4, "RUP Installer Configuration Tasks". Before the **Starting All Servers** task, the **Verifying Node Manager and OPMN Status** configuration task checks for access to the Node Manager and the OPMN control process. This should fail because you manually shut down these processes prior to starting RUP Installer. Do not cancel and exit out of RUP Installer in response to this task.

Table 5–4   (Cont.) RUP Installer Screen Sequence

Screen	Description and Action Required
Configuration Progress (continued)	After this task fails, follow these steps:

1. Start the Node Manager on all hosts that are part of the Oracle Fusion Applications provisioned system. For more information, see "Start Node Manager" in *Oracle Fusion Applications Administrator's Guide*.

2. Restart the OPMN server for BI and GOP, and the OPMN server plus managed processes for Web Tier. This is similar to the `stop` steps described in Section 5.3.3.2, "Stop the Node Manager and the OPMN Control Process", except that for BI and GOP, you must start only the OPMN server itself, while for Web Tier, you should start OPMN and all processes that it manages. If you run the Web Tier (OHS) installed with the Oracle Fusion Applications middle tier, you can start it using the following steps. If you run the Web Tier on a separate machine, you may be able to run the steps below on the other machine. In either case, ensure that Web Tier (OHS) is up at this point. Note that the OPMN server for GOP should be started from the machine that hosts the Supply Chain Management domain.

Example for BI: (note the usage of `start` instead of `startall`)

```
cd APPLICATIONS_CONFIG/BIInstance/bin
./opmnctl start
```

Example for GOP: (note the usage of `start` instead of `startall`)

```
cd APPLICATIONS_CONFIG/gop_1/bin
./opmnctl start
```

Example for Web Tier:

```
cd APPLICATIONS_CONFIG/CommonDomain_webtier/bin
./opmnctl startall
```

For more information about the location of `APPLICATIONS_CONFIG`, see Section 5.2.1, "Before You Begin".

The BI processes managed by OPMN are started by RUP installer in the Start All Servers configuration task. The GOP processes managed by OPMN can be started by an administrative user from the GOP home page in Oracle Enterprise Manager after RUP installer completes.

3. Fix any other environment issues before retrying the session. If RUP Installer exits for any reason, make sure that all node managers and OPMN processes are running. Contact Oracle Support Services to proceed out of this step if you have unresolved environment issues.

4. After you start the services, click **Retry** to proceed to the **Starting All Servers** task. If the starting of servers times out, see Section 5.5.16, "Failures During Starting All Servers".

No additional user action is required in the Configuration Progress screen unless a failure occurs. For more information, see Section 5.5.3, "General Troubleshooting During the Configuration Phase".

Table 5–4   (Cont.) RUP Installer Screen Sequence

Screen	Description and Action Required
Installation Complete	Summarizes the installation just completed. If you want to save this configuration to a response file, click **Save**. For more information, see "How Response Files Work" in the *Oracle Database Installation Guide 11g Release 2 (11.2) for Linux*.
	To complete a successful installation, click **Finish**. The **Finish** button is activated only if all mandatory configuration tasks completed successfully. If you want to rerun this session to resolve failed configuration tasks, click **Cancel.**

5.4.2 Complete the Post Installation Tasks

Perform the following required manual steps after RUP Installer completes successfully:

1. Copy the generated OHS configuration `<location>` elements. If your OHS is scaled out, then the following steps must be repeated for each additional OHS server.

    a. The generated OHS configuration snippets are under *FA_ORACLE_ HOME*/admin/OHS/patched_moduleconf. For each product family file under that directory, identify all `<location>` elements. Copy and paste these elements to the corresponding file under *APPLICATIONS_ BASE*/instance/CommonDomain_ webtier/config/OHS/ohs1/moduleconf.

    Further customization of the generated OHS configuration `<location>` is needed if any of your Oracle Fusion Applications domains are scaled out. For more information, see "Oracle HTTP Server Configuration" in the *Oracle Fusion Applications Enterprise Deployment Guide*. The generated OHS configuration snippet only contains one server. If there are additional servers in the cluster, you must add the additional server host and port. For example, the following example shows one server.

    ```
    <Location /icCnSetupCreditRulesPublicService >
    SetHandler weblogic-handler
    WebLogicCluster server_name_1:9809
    </Location>
    ```

    The following example has been updated for two servers.

    ```
    <Location /icCnSetupCreditRulesPublicService >
    SetHandler weblogic-handler
    WebLogicCluster server_name_1:9809,server_name_2:9804
    </Location>
    ```

    b. Stop and start the OHS server.

    c. Verify that the new context roots are accessible through an internet browser. The context roots in the location elements indicate that requests are rerouted to the host and port specified in the location element. The URL that can be used to verify the context root depends on the application that hosts the context root. No standard pattern can be followed.

2. Follow these steps to manually deploy `sca_UpdateSOAMDS_rev1.0.jar` SOA composite to every domain:

    a. Access the WLST shell.

```
(UNIX) SOA_ORACLE_HOME/common/bin/wlst.sh
(Windows) SOA_ORACLE_HOME\common\bin\wlst.cmd
```

b. Deploy the composite using the `sca_deployComposite` WLST command to the SOA server of each domain. This composite is located under *APPLICATIONS_BASE*/`fusionapps/atgpf/pcbpel/composite/sca_ UpdateSOAMDS_rev1.0.jar`.

```
sca_deployComposite(serverURL, sarLocation, overwrite=true)
```

Where:

- **serverURL** is the URL of the server that hosts the SOA Infrastructure application (for example, `http://hostname:8001`).

- **sarLocation** is the absolute path of the SAR file or the ZIP file that bundles multiple SAR files, MAR files, or both. Since the installer copies the `UpdateSOAMDS` composite to *APPLICATIONS_ BASE*/`fusionapps/atgpf/pcbpel/composite/` in the target system, the `sarLocation` argument should be set to the absolute path of the composite at that location, as shown in the example.

- **overwrite** specifies whether to overwrite a currently deployed SOA composite.

Example:

```
sca_deployComposite('http://abc10:8001', 'APPLICATIONS_
BASE/fusionapps/atgpf/pcbpel/composite/sca_UpdateSOAMDS_rev1.0.jar',
overwrite=true)
```

c. You must run `UpdateSOAMDS` composite if you made any flexfield changes. For more information, see "Task: Synchronizing Customized Flexfields in the SOA MDS Repository" in the *Oracle Fusion Applications Extensibility Guide*.

3. Update the `essbase.cfg` file by performing the following steps:

a. Back up `essbase.cfg` to `essbase.cfg.copy`.

b. Shut down the agent `essbaseserver1` using the following commands:

```
./opmnctl stopproc ias-component=essbaseserver1
./opmnctl status
```

c. Add the line `JAVAMAXOUTLINES 128` to `essbase.cfg`.

- Go to this directory to *FA_MW_ HOME*/`localdomain/BIInstance/Essbase/essbaseserver1/bi n`

- Edit `essbase.cfg` to add a line that contains JAVAMAXOUTLINES 128.

d. Start the agent `essbaseserver1` using the following commands:.

```
./opmnctl startproc ias-component=essbaseserver1
./opmnctl status
```

4. Perform the following steps to move the `userpref_currencies.xml` file.

a. Review the following file:

```
APPLICATIONS_
BASE/instance/BIInstance/config/OracleBIPresentationServicesComponent/corea
pplication_obips1/instanceconfig.xml
```

b. Check if the file contains the following element:

```
<UserprefCurrenciesConfigFile>[BI InstanceHome]
/config/OracleBIPresentationServicesComponent/coreapplication_
obips1/userpref_currencies_OTBI.xml</UserprefCurrenciesConfigFile>
```

c. If this element is not available, perform the following steps in this section. If this element is available, no further action is required.

d. Back up the file, *APPLICATIONS_ BASE*/instance/BIInstance/config/OracleBIPresentationServic esComponent/coreapplication_obips1/userpref_currencies.xml to userpref_currencies.xml.backup.

e. Copy the file, *BI_ORACLE_ HOME*/bifoundation/admin/config/OracleBIPresentationService sComponent to *BI_INSTANCE_ HOME*/config/OracleBIPresentationServicesComponent/coreappl ication_obips1/userpref_currencies.xml.

For example, copy from:

```
/u01/APPTOP/fusionapps/bi/bifoundation/admin/config/Oracle
BIPresentationServicesComponent/userpref_currencies_
OTBI.xml
```

to:

```
/u01/APPTOP/instance/BIInstance/config/OracleBIPresentatio
nServicesComponent/coreapplication_obips1/userpref_
currencies.xml.
```

If you are using local domains, replace APPTOP with the local domain directory.

f. Bounce the coreapplication_obis1 server.

5. Confirm that all deployments were successful by reviewing the Diagnostics report and log files. For more information, see Section 3.5.5, "Diagnostics Report".

6. Confirm there are no unresolved errors or exceptions in the log files. For information about resolving errors, see Section 5.5, "Troubleshoot RUP Installer Sessions".

7. Confirm that all relevant Managed Servers have a RUNNING status.

8. Verify that all deployed applications are up and running. You can check this from Fusion Applications Control, or by reviewing the server side log files. For more information, see "Starting Fusion Applications Control" in the *Oracle Fusion Applications Administrator's Guide* or Section 5.5.1, "RUP Installer Log File Directories".

9. Perform the following steps to start or stop the GOP processes. Note that the opmnctl process for gop_1 should only be started on the host machine which contains the AdvancedPlanning Managed server. Do not start it on the primordial host.

a. Proceed to Step b if your GOP processes have been previously configured and have run before.

If you are starting GOP processes for the first time, confirm that a datasource exists, in the form of XML files, under the *APPLICATIONS_ BASE*/instance/gop_

1/GOP/GlobalOrderPromisingServer1/datasource directory. Then run the RefreshOpDatastore ESS job.

b. Log in to Fusion Applications Control. For more information, see "Starting Fusion Applications Control" in the *Oracle Fusion Applications Administrator's Guide*.

c. Access GOP by navigating to **Oracle Fusion Supply Chain Management**, then **Global Order Promising**, then **GlobalOrderPromisingServer1**.

d. Click **GlobalOrderPromisingServer1** to open the GlobalOrderPromisingServer1 page.

e. Select **Control** from the menu, then **Start Up**.

10. Follow this step if you have customized BI Publisher reports.

Reload custom templates for BI Publisher reports on Oracle-delivered BI Publisher reports by following the steps in "Task: Upload the Template File to the Report Definition" in the *Oracle Fusion Applications Extensibility Guide*.

11. Review the JAZN Analyze report for potential conflicts and deletions that are not patched automatically by RUP Installer.

FA_ORACLE_HOME/admin/JAZN/*stripe*/delta/report.txt

The *stripe* is crm, fscm, hcm, or obi.

Review the Modification section of the report to see the roles that RUP Installer did not update. For each conflict that displays in this report, you must evaluate and manually patch the role by using APM. For more information, see "Upgrading Oracle Fusion Applications Policies" in the *Oracle Fusion Middleware Oracle Authorization Policy Manager Administrator's Guide (Oracle Fusion Applications Edition)*.

The following example shows a typical Application Role conflict that has been modified by both the patch and production, therefore it is not applied by RUP Installer.

```
MODIFICATION CONFLICTS
Artifact type: Application Role
Artifact Name: OBIA_PARTNER_CHANNEL_ADMINISTRATIVE_ANALYSIS_DUTY
Description: This artifact is modified at attribute level in patch version and
also in production.
```

Note the location of the following files for reference when using APM:

- Location of baseline files, where stripe is crm, fscm, hcm, or obi:

    FA_ORACLE_HOME/admin/JAZN/*stripe*/baseline

- Location of patch files for fscm, crm, and hcm stripes:

  FA_ORACLE_HOME/stripe/deploy/system-jazn-data.xml

- Location of patch files for the obi stripe:

  FA_ORACLE_HOME/com/acr/security/jazn/bip_jazn-data.xml

12. If the RUP contains ODI artifacts, you must manually drop the work tables from the schema, FUSION_ODI_STAGE.

- Connect to the Oracle Fusion Applications database with the correct privilege.

- Drop all tables that begin with E$ from the FUSION_ODI_STAGE schema.

13. Apply all mandatory post installation patches and follow any post installation steps mentioned in the "Applying Patches" section of Oracle Fusion Applications release notes.

14. Run the script `enable_partition_attr_val.sql` to improve the query and crawl performance. This step is optional.

The script `enable_partition_attr_val.sql` may take several hours to complete, depending on the number of documents that have been previously indexed, and the number of custom attributes. This script can be run ONLINE.

Follow these steps to run the script `enable_partition_attr_val.sql`:

a. Start SQL*Plus and connect as the `SYS` user.

b. Run the following script:

   SES_ORACLE_HOME/search/admin/scripts/enable_partition_attr_val.sql

15. Activate the schedules by running the following commands.

```
SES_ORACLE_HOME/bin/searchadmin -p ses_Admin_Password  -c
http://ses_Admin_Host:ses_Admin_Port/search/api/admin/AdminService
activate schedule -n schedule_Name

SES_ORACLE_HOME/bin/searchadmin -c
http://sesHost:sesPort/search/api/admin/AdminService -p ses_Admin_Password
activate indexOptimizer
```

The variables, *ses_Admin_Host* and *ses_Admin_Port*, refer to the host and port of the **search_server1** Managed Server or SES cluster

The variable, *ses_Admin_Password*, is the SEARCHSYS database schema password, which is the same as the SES Admin screen.

The `-p` on the command line is optional. If you do not use it, you will be prompted for it.

16. For security, you must perform the following tasks in the IDM domain:

- Disable anonymous binds to Oracle Virtual Directory's LDAP ports

- Disable Oracle Virtual Directory ACLs

You perform both tasks at the same time by running the `idmConfigTool` with the `-disableOVDAccessConfig` option. Proceed as follows:

a. Set the environment variables *MW_HOME*, *IAM_HOME*, *JAVA_HOME*, and *ORACLE_HOME* as shown in the following examples:

```
setenv MW_HOME /u01/oid
setenv IAM_ORACLE_HOME /u01/oim/oim_home
```

```
setenv JAVA_HOME /u01/oim/jrockit-jdk1.6.0_24
setenv ORACLE_HOME /u01/oim/oim_home
```

b. Stop Oracle Virtual Directory as described in "Starting and Stopping Oracle Identity Management Components" in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management (Oracle Fusion Applications Edition).*

c. Create a properties file called `disableOVDAcces.prop`, with the following contents:

```
ovd.host:ovdhost1.mycompany.com
ovd.port:1234
ovd.binddn:cn=orcladmin
ovd.password:password
ovd.ssl:true
```

Where:

– `ovd.host` is the name of the host that the Oracle Virtual Directory server runs on.

– `ovd.port` is the Oracle Virtual Directory https port.

– `ovd.binddn` is the name of the Oracle Virtual Directory administrative user.

– `ovd.ssl` indicates that you are communicating with Oracle Virtual Directory using the https protocol.

d. Disable Oracle Virtual Directory ACLs and anonymous binds to Oracle Virtual Directory LDAP ports using the command `idmConfigTool` which is located in the *IAM_ORACLE_HOME*/idmtools/bin directory.

Note: When you run the `idmConfigTool`, it creates or appends to the file `idmDomainConfig.param`. This file is generated in the same directory that the `idmConfigTool` is run from. To ensure that the same file is appended to each time the tool is run, always run the `idmConfigTool` from the *IAM_ORACLE_HOME*/idmtools/bin directory.

```
(Unix) idmConfigTool.sh -disableOVDAccessConfig input_file=properties_file
```

```
(Windows) idmConfigTool.bat -disableOVDAccessConfig input_file=properties_
file
```

For example:

```
idmConfigTool.sh -disableOVDAccessConfig input_file=disableOVDAcces.prop
```

e. Check the log file for any errors or warnings and correct them. Output is saved in a file named `automation.log`, which is created in the directory where you run the tool.

f. Restart Oracle Virtual Directory as described in "Starting and Stopping Oracle Identity Management Components" in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management (Oracle Fusion Applications Edition).*

Repeat Steps a through f for each Oracle Virtual Directory instance, changing the values in the property file as necessary.

17. In Oracle Fusion Applications 11.1.3.0.0, Oracle moved some tables and indexes from the FUSION schema into different tablespaces. Starting with 11.1.3.0.0, those tables that are seeded with rows by Oracle reside in the FUSION_TS_SEED tablespace and those that are not seeded with rows do not reside in the FUSION_TS_SEED tablespace. This was done to leverage the Transportable Tablespace database feature.

Run the following script to move these objects into new tablespaces so that the tablespace assignment of FUSION objects in your database matches those of a freshly installed RUP2 database.

From the operating system, run the following command:

```
sqlplus FUSION_schema/FUSION_password APPLICATIONS_BASE/com/acr/db/sql/acr_
tablespace_move.sql
```

If you have not customized the FUSION tablespaces, you must run this script as it is delivered by Oracle. If you customized the tablespaces in which the FUSION-owned objects reside, then you may edit this script before running it to match the customizations that you implemented regarding tablespace assignment for FUSION objects.

Oracle recommends that you save the output of the script and review it for any errors. For example, you may run out of space in one or more tablespaces, in which case you must refer to the Oracle Database Administrators Guide, rectify the situation, and rerun the script.

18. If you are deploying Oracle Business Intelligence Applications, then you must perform the post-installation or upgrade steps specified in "Roadmap for Installing, Upgrading, and Setting Up Oracle BI Applications" in *Oracle Fusion Middleware Installation and Configuration Guide for Oracle Business Intelligence Applications*.

19. If you have installed any languages in addition to US English, you must upgrade each installed language using Language Pack Installer. For more information, see Chapter 6, "Maintaining Oracle Fusion Applications Languages".

5.5 Troubleshoot RUP Installer Sessions

This section provides information to assist you in troubleshooting RUP Installer sessions. It contains the following topics:

- RUP Installer Log File Directories
- Troubleshooting Failures During the Installation Phase
  - Invalid Oracle Home
  - Error in Writing to File, Text File Busy
  - Inventory Pointer File is Empty
- General Troubleshooting During the Configuration Phase
- The Next Button Is Not Enabled During Configuration Tasks
- Error Finding WEBLOGIC_HOME
- Error During Bootstrapping Patch Manager
- Troubleshooting Applying Middleware Patches

- [Failure During Applying Middleware Patch Sets](#)

- [EditTimedOutException Error During Online Preverification](#)

- [Troubleshooting Loading Database Components](#)

- [LdapServerCheck Failure](#)

- [Troubleshooting Deployment of Applications Policies](#)

- [Failure during Applying OAM Configuration](#)

- [Webcat Patch File Creation Failure](#)

- [Failure During Deployment of BI Publisher Artifacts](#)

- [Failures During Starting All Servers](#)

- [Failure During IPM Import](#)

- [Merging SOA Composite JDeveloper Customizations While Installing a RUP](#)

- [Troubleshooting SOA Composite Deployment Failures](#)

- [Failure During Applying BI Metadata Updates](#)

- [AttachHome Script Hangs](#)

- [The runInstaller.sh -updateHomeDeps Command Hangs](#)

- [Verify Your Installation](#)

RUP Installer calls Oracle Fusion Applications Patch Manager during the Load Database Components task. For additional information about troubleshooting Oracle Fusion Applications Patch Manager sessions, see Chapter 11, "Monitoring and Troubleshooting Patches".

5.5.1 RUP Installer Log File Directories

Table 5–5 contains a list of log directories for RUP Installer activities.

Table 5–5   Log Directories for RUP Installer Activities

Log directory name	Generated from...
oracle_inventory/logs	Installation phase
FA_ORACLE_ HOME/admin/FUSION/log/fapatch/fapatch_ 11.1.3.0.0/*timestamp*	Top level log directory which contains the main RUP installer log file
FA_ORACLE_ HOME/admin/FUSION/log/fapatch/fapatch_ 11.1.3.0.0/ARCHIVE/*timestamp*	Top level log directory where log files are moved when you retry the RUP installation session
FA_ORACLE_ HOME/admin/FUSION/log/fapatch/fapatch_ 11.1.3.0.0/PatchManager_DBPatch	Database upload configuration task after failure or completion.
FA_ORACLE_ HOME/admin/FUSION/log/fapatch/fapatch_ 11.1.3.0.0/StartStop	StartStop utility. Note that server logs are located under respective domains. For example, the AdminServer log for CommonDomain is under *APPLICATIONS_ BASE*/instance/domains/*ho stname*/CommonDomain/serv ers/AdminServer/logs.

Table 5–5   (Cont.) Log Directories for RUP Installer Activities

Log directory name	Generated from...
FA_ORACLE_HOME/admin/FUSION/log/fapatch/fapatch_11.1.3.0.0/soalogs	Processing SOA artifacts. Note that SOA server logs are located under respective domains. For example, the SOA server logs for CommonDomain are under *APPLICATIONS_BASE*/instance/domains/*hostname*/CommonDomain/servers/soa_server1/logs. For more information, see Section 5.5.19.1, "SOA Composite Log Files".

During the execution of configuration tasks, log files are created under the *FA_ORACLE_HOME*/admin/FUSION/log/fapatch/fapatch_*releasenumber* directory. During the execution of the database upload configuration task, log files are created under *FA_ORACLE_HOME*/admin/FUSION/log. Upon completion or failure of the database upload, the log files move to the *FA_ORACLE_HOME*/admin/FUSION/log/fapatch/fapatch_*releasenumber*/PatchManager_DBPatch directory. The current *releasenumber* is 11.1.3.0.0 for RUP2.

5.5.2 Troubleshooting Failures During the Installation Phase

RUP Installer backs up the contents of the *FA_ORACLE_HOME*/patchsettop directory after it completes the installation phase. The backup directory is *FA_ORACLE_HOME*/patchsettop/backup/*version*/*language*/*timestamp*. For RUP3, the directory is *FA_ORACLE_HOME*/patchsettop/backup/11.1.3.0.0/en_US/*timestamp*. When RUP Installer restarts after a failure, it ensures that the contents in the *FA_ORACLE_HOME*/patchsettop directory are relevant for the current session. When RUP Installer exits the installation phase, it deletes any existing content in the *FA_ORACLE_HOME*/patchsettop directory.

Follow these steps when an error occurs during the installation phase:

1. Click **Cancel** to exit RUP Installer.

2. Review the log files to determine the cause of the failure. The log files reside in oracle_inventory/logs/install*timestamp*.log.

3. Resolve the cause of the failure.

4. Start RUP Installer using the same command syntax that you used for the previous incomplete installation. For more information, see Section 5.4.1, "Perform the Installation". After canceling the previous installation and starting again, you must choose to continue with the previous failed installation by clicking **Yes** on the Checkpoint Dialog. If the error is not recoverable, you can restore and restart from backup.

5. If you choose to continue with the failed installation, RUP Installer opens at the screen where it was canceled. When canceled during the copy action, it relaunches in the Installation Summary screen. Click **Next** to navigate through the Installation Summary screen. When the Installation Progress screen displays, click **Install** to start the installation again.

Troubleshooting steps are described for the following specific failures that may occur during the installation phase:

- Invalid Oracle Home
- Error in Writing to File, Text File Busy
- Inventory Pointer File is Empty

5.5.2.1 Invalid Oracle Home

In the Installation Location page, you receive a message about entering an invalid Oracle home, even though the location displayed on the page is correct. RUP Installer reads `/etc/oraInst.loc` to determine the location of the central inventory. Review the following settings:

- Ensure that the `/etc/oraInst.loc` file on the machine where you are running RUP Installer is pointing to the correct central inventory location.

- Ensure that the *FA_ORACLE_HOME* matches the values provided during provisioning. If a `/net/location` was provided as the Oracle home location during provisioning, the same `/net/location` that corresponds to *FA_ORACLE_HOME* should be provided during the RUP Installation.

5.5.2.2 Error in Writing to File, Text File Busy

During the installation phase of RUP Installer, you receive the following message on a Unix platform.

```
Error in writing to file
'/server01/APPLICATIONS_BASE/fusionapps/applications/lcm/ad/bin/adctrl'
(Text file busy)
```

To resolve this issue, perform the following steps.

1. Run the `lsof` command using the full directory path of the file that is busy.

   ```
   /usr/bin/lsof full_path_to_file
   ```

2. You should receive a list of process ids that are using the file. Kill each process using the appropriate command for your operating system.

3. After all processes are no longer running, click **Continue** in RUP Installer.

5.5.2.3 Inventory Pointer File is Empty

After running RUP Installer, the contents of `oraInst.loc` were removed.

RUP Installer always tries to copy the inventory pointer file specified by the `-invPtrLoc` option to the Oracle home on which the RUP is to be installed. If you specify an incorrect path for the `-invPtrLoc` file, the inventory pointer file could result in being an empty file. There are three possible solutions to this issue:

- For best results, if you are using the `-invPtrLoc` option, use it with this value: *FA_ORACLE_HOME*`/oraInst.loc`. This avoids a situation where you may inadvertently exclude part of the directory path to the file, as in the case of using a mapped drive. For example, if Oracle home is registered in inventory with a `/net` path, such as `/net/home/oraInst.loc`, and you provide `/home/oraInst.loc` to the `invPtrLoc` option, the installer interprets the two paths as different. The end result is an empty inventory pointer file.

- If *FA_ORACLE_HOME* is registered in central inventory with a `/net` path, then you must include `/net` when specifying the location of the inventory pointer file with

the -invPtrLoc option, for example, -invPtrLoc /net/*directory_path*/oraInst.loc.

- Restore from a backup copy of your oraInst.loc file in case the original file is damaged.

- You can recover from this error by creating a new oraInst.loc. See the "Creating the oraInst.loc File" section in the relevant Oracle Database installation guide, for example, *Oracle Database Installation Guide, 11g Release 2 (11.2) for Linux*.

  Then click **Retry**.

5.5.3 General Troubleshooting During the Configuration Phase

RUP Installer can be restarted to rerun all failed configuration tasks as well as those tasks that were not started from the previous session. When a configuration task or step fails, the Configuration Progress screen displays the location of the log file and the exception that caused the failure. You can also view the content of the log files that appear at the bottom of the screen to obtain detailed information to assist in diagnosing the cause of the failure.

If one or more failures occur during the configuration phase, the following message displays after the final configuration task is complete:

Configuration is completed with errors, exit the installer by clicking the 'Cancel' button and retry the failed configurations.

Perform the following steps to rerun RUP Installer and retry the failed configuration tasks:

1. Click **Cancel** to exit RUP Installer.

2. Resolve the issues that caused the failure.

3. Start RUP Installer using the same command syntax that you used for the previous incomplete installation. For more information, see Section 5.4.1, "Perform the Installation".

4. A pop up dialog displays, asking if you want to continue the previous incomplete installation. Select **Yes** to continue the previous session. If you select **No**, RUP Installer starts from the beginning and it will fail, indicating that a RUP cannot be installed again in the same environment. You would then need to restore from your backup and restart the RUP installation.

5. The Configuration Progress screen displays only the failed and remaining configuration tasks, and then runs these tasks.

6. Assuming all configuration tasks complete successfully, click **Next** to go to the Installation Complete screen and then click **Finish** to end the session. If a configuration task fails again and you want to attempt to run the session again, click **Cancel** to save the session.

5.5.4 The Next Button Is Not Enabled During Configuration Tasks

On the Configuration Progress page of RUP Installer, the **Next** button is enabled only when all configuration tasks are successful.

If you see that all your configurations are complete, and the **Next** button is not enabled, you encountered a configuration failure and continued on to the next configuration. In this case, you must retry the failed configurations by following these steps:

1. On the Configuration Progress page of the RUP Installer, click **Cancel**.

2. Restart RUP Installer. All failed configuration actions or steps are re-executed upon restart. For more information, see Section 5.5.3, "General Troubleshooting During the Configuration Phase".

As long as a configuration task is not successful, the **Next** button remains disabled. It may be necessary to repeat the cancel and restart procedure until all configuration tasks are successful.

5.5.5 Error Finding WEBLOGIC_HOME

On the Configuration Progress page of RUP Installer, a `java.lang.RuntimeException:: error in finding weblogic.Home` error may occur. The Oracle WebLogic Server class path may be corrupted.

Follow these steps to resolve this issue:

1. On the Configuration Progress page of RUP Installer, click **Cancel**.

2. Set the WEBLOGIC_HOME in the CLASSPATH parameter explicitly. For example:

   ```
   CLASSPATH=WLS_HOME/server/lib/weblogic.jar:$CLASSPATH
   ```

3. Restart RUP Installer. All failed configuration actions or steps rerun upon restart.

5.5.6 Error During Bootstrapping Patch Manager

An error during the **Bootstrapping Patch Manager** configuration task normally occurs only when the database is down. Ensure that the database is up and running. You can review the related log files in this location:

FA_ORACLE_HOME/admin/FUSION/log/FAPatchManager_bootstrap_*timestamp*.log

5.5.7 Troubleshooting Applying Middleware Patches

If an error occurs during the **Applying Pre-PSA Middleware Patches** or **Applying Post-PSA Middleware Patches** configuration tasks, review the log file in the relevant location:

*FA_ORACLE_HOME/*admin/FUSION/log/fapatch/fapatch_11.1.3.0.0/ApplyPrePSAMiddlewarePatches*timestamp*.log

*FA_ORACLE_HOME/*admin/FUSION/log/fapatch/fapatch_11.1.3.0.0/ApplyPostPSAMiddlewarePatches*timestamp*.log

For specific OPatch failures, go to each of the individual Oracle home directories to find the details of the OPatch errors. For example, for a SOA failure, go to *APPLICATIONS_BASE/*fusionapps/soa/cfgtoollogs/opatch.

5.5.8 Failure During Applying Middleware Patch Sets

Perform the following steps if the following error occurs during **Applying Middleware Patch Sets:**

```
Jobs failed during Applying Middleware Patchsets: [[{ Job ID 8 (seq[12]
OUIINSTALLER:odi):
```

1. Confirm that you have followed the instructions in Section 5.3.2, "Apply Mandatory Prerequisite Patches", Step 6.

2. If you are installing the RUP in an Oracle VM environment, ensure that ODI Standalone Agent is installed. If this is not installed, refer to "Installing Oracle Data Integrator (ODI) Standalone Agent for a Successful RUP Installation" in Oracle Fusion Applications release notes, 11g Release 1, Update 2 (11.1.3.0.0).

5.5.9 EditTimedOutException Error During Online Preverification

If you receive the following error during preverification, you may have to manually release the edit session. For more information, see Section 11.3.8, "Resolving an EditTimedOutException Error".

```
weblogic.management.mbeanservers.edit.EditTimedOutException
```

5.5.10 Troubleshooting Loading Database Components

This section contains information about troubleshooting issues that can occur during the **Loading Database Components** configuration task. Depending on the type of failure, you may need to review one or more of the log files in the following locations:

- *FA_ORACLE_HOME*/admin/FUSION/log/fapatch/fapatch_
  11.1.3.0.0/PatchManager_DBPatch/

  - FAPatchManager_apply_*timestamp*.log

  - adpatch_apply_*timestamp*.log

  - adpatch_apply_*timestamp_workerum*.log

- *ATGPF_HOME/*admin/FUSION/log

5.5.10.1 Error While Loading Database Tasks

When RUP Installer notifies you that one or more database workers failed during the **Loading Database Components** configuration task, you must start AD Controller to manage the failed workers. For more information, see Section 11.5, "Troubleshooting Patching Sessions for Database Content". After you resolve the issue that caused the workers to fail and you restart the failed worker, click **OK** in the dialog box and RUP Installer continues processing.

5.5.10.2 Database Failure While Loading Database Components

If your database goes down while RUP Installer is running the **Loading Database Components** configuration task, the options to **Abort** or **Retry** display. If you simply bring the database up and then click **Retry**, you may encounter the following error:

```
Failed to connect to the database as fusion with error:
No more data to read from socket
```

Perform the following steps to recover from this error:

1. Force the database patching session to fail.

   ```
   (Unix) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh -forcefail
   (Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd -forcefail
   ```

2. Start AD Controller.

   ```
   (UNIX) FA_ORACLE_HOME/lcm/ad/bin/adctrl.sh
   (Windows) FA_ORACLE_HOME\lcm\ad\bin\adctrl.cmd
   ```

   For more information, see Section 11.5.1, "Starting AD Controller".

3. Follow this sequence of steps in AD Controller to manage the workers:

a. Select **Tell manager that a worker failed its job** and enter **All** for all workers.

b. Select **Tell worker to quit** and enter **All** for all workers. Note that this does not kill the workers. It sends a command to the worker to shutdown after it completes the current task.

c. Wait for all workers to complete their tasks and shut down normally.

d. If there are still some worker processes that do not shut down, kill those processes manually by selecting **Tell manager that a worker failed its job**. Then select **Tell manager that a worker acknowledges quit** and enter **All** for all workers.

e. From your operating system, check for processes that are running `fapmgr`, `javaworker`, `adpatch`, `adadmin`, `sqlplus`, and `adworker`. If any exist, terminate them from your operating system. For more information, see

f. Select **Tell worker to restart a failed job** and enter **All** for all workers.

4. Select **Cancel** to stop the session and restart RUP Installer.

5.5.10.3 AutoPatch Validation Fails

If AutoPatch validation fails, you receive this message:

```
An active adpatch or adadmin session was found. Complete or
terminate the active session to allow fapmgr to proceed.
```

Follow these steps to resolve this error:

1. Run the `fapmgr forcefail` command to update the patching tables.

   ```
   (UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh forcefail [-logfile log file name]
   [-loglevel level]

   (Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd forcefail [-logfile log file
   name] [-loglevel level]
   ```

2. Run the `fapmgr abort` command from *FA_ORACLE_HOME* to find out if an Oracle Fusion Applications Patch Manager must be cleaned up.

   ```
   (UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh abort [-logfile log file name]
   [-logLevel level]

   (Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd abort [-logfile log file name]
   [-logLevel level]
   ```

   If this command finds no failed session, proceed to Step 3.

3. Run the following commands from *ATGPF_ORACLE_HOME* to abandon any Applications Core patching sessions or AD Administration sessions that may be running:

   ```
   (Unix) ATGPF_ORACLE_HOME/lcm/ad/bin/adpatch.sh abandon=y interactive=n
   defaultsfile=ATGPF_ORACLE_HOME/admin/TWO_TASK/defaults_file_name.txt

   (Unix) ATGPF_ORACLE_HOME/lcm/ad/bin/adadmin.sh abandon=y interactive=n
   defaultsfile=ATGPF_ORACLE_HOME/admin/TWO_TASK/defaults_file_name.txt

   (Windows) ATGPF_ORACLE_HOME/lcm/ad/bin/adpatch.exe abandon=y interactive=n
   defaultsfile=ATGPF_ORACLE_HOME\admin\TWO_TASK\defaults_file_name.txt

   (Windows) ATGPF_ORACLE_HOME\lcm\ad\bin\adadmin.cmd abandon=y interactive=n
   defaultsfile=ATGPF_ORACLE_HOME\admin\TWO_TASK\defaults_file_name.txt
   ```

5.5.11 LdapServerCheck Failure

If the OPSS Security Store is not running before RUP Installer starts, the related configuration task will fail. Even if you start this server after you notice the failure, the configuration task fails again, with the following error:

```
Retry of step
"oracle.as.install.fapatchconfig.plugin.impl.LdapServerCheck" failed.
```

Follow these steps to recover:

1. **Abort** the failed configuration task.

2. Select **Cancel** to end the RUP Installer session.

3. Start the OPSS Security Store. For more information, see "Starting and Stopping Oracle Internet Directory" in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management (Oracle Fusion Applications Edition)*.

4. Start a new RUP Installer session. The installer resumes with the remaining tasks because you selected **Cancel**, which saves the session.

5.5.12 Troubleshooting Deployment of Applications Policies

This section contains information about troubleshooting issues that may occur during the **Deploying Application Policies** configuration task. Log files for this task may be found in this location:

```
FA_ORACLE_HOME/admin/FUSION/log/fapatch/fapatch_
11.1.3.0.0/fapatch_timestamp.log
```

5.5.12.1 Failure During Deployment of Applications Policies

When a failure occurs during **Deploying Application Policies**, you must restore only the stripe or system policy that failed from your backup. Use the OPSS `migrateSecurityStore` command with the appropriate source and destination arguments to perform the restore. Do not restore a stripe that has not failed. Review the log file to determine the cause of the failure. If needed, you can also review the log file that is specifically generated by each stripe. These following log files are located under the main log directory, *FA_ORACLE_HOME*/admin/FUSION/log/fapatch/fapatch_11.1.3.0.0/*timestamp*:

- `fapatch_CRMJaznAnalysis_timestamp`.log

- `fapatch_FSCMJaznAnalysis_timestamp`.log

- `fapatch_HCMJaznAnalysis_timestamp`.log

- `fapatch_OBIJaznAnalysis_timestamp`.log

After you resolve the issue, restart RUP Installer by either selecting **Retry** in the same session or by exiting RUP Installer and restarting it.

For more information, see "Migrating with the Script migrateSecurityStore" in the *Oracle Fusion Middleware Application Security Guide*.

5.5.12.2 Stripe Version Mismatch in Applications Policies

After the deployment of Applications Policies, a version check is performed, to ensure that the version of each stripe was updated successfully in OID. If the version of a stripe is incorrect, an error about a version mismatch is reported.

To resolve this issue, you may need a fix from Oracle Support to retry the deployment after you restore your policy store. Use the OPSS `migrateSecurityStore` command with the appropriate source and destination arguments. Do not restore a stripe that has not failed.

For more information, see "Migrating with the Script migrateSecurityStore" in the *Oracle Fusion Middleware Application Security Guide*.

5.5.12.3 IDM Server Failure During Deployment of Applications Policies

If the IDM Server goes down during the deployment of applications policies, the deployment fails. Even if the **Retry** button is enabled, RUP Installer does not allow a retry after this type of failure. You must instead click **Cancel** and restart RUP Installer.

5.5.12.4 JAZN Policy Stripe Version Validation Failure

Read only permission on a `.tmp` file could result in a failure during JAZN policy stripe validation. This file is created by the Oracle Enterprise Agent, with a file name such as, `/tmp/pki_data1967998276.lck.tmp`. The file is owned by `emcadm`, so the policy version validation fails. Because the policy upload completes before version validation starts, you can click **Continue** to proceed to the next task.

5.5.12.5 migrateSecurityStore Command Fails

While running the WLST command `migrateSecurityStore` to backup applications and system policies, the command fails with the following error:

```
Command FAILED, Reason: JPS-00056: Failed to create identity store service
instance idstore.ldap.provider:idstore.ldap.
Reason: java.lang.ClassNotFoundException:
oracle.security.jps.wls.internal.idstore.WlsLdapIdStoreConfigProvider.
```

To resolve this error, remove the entry, `<serviceInstanceRef ref="idstore.ldap"/>`, as described in Step 4 in Section 5.3.4.3, "Back Up Applications and System Policies".

5.5.13 Failure during Applying OAM Configuration

If the **Applying OAM Configuration** task fails with the following error:

```
[ecid: 0000JVgds_DAtHc5ljO5yZ1Fq^T6000004,0] Cannot find applications
matching name [ webcenter* ].[[
oracle.apps.ad.common.exception.ADException: Cannot find applications
matching name [ webcenter* ].
at
oracle.apps.ad.common.taxonomy.WLSUtil.getApplicationsStartingWith(WLSUtil.java:92
5)
at
oracle.apps.ad.fapmgr.sdk.FAPManagerSDK.getServerDetailsForWebcenterApp(FAPManager
SDK.java:2977)
```

Perform this workaround to run `oamcfgtool.jar` manually from the command-line. Note that the parameters in brackets <> must be replaced with valid values first.:

```
$ setenv APPTOP <Apptop location>

$ cd ${APPTOP}/fusionapps/oracle_common/modules/oracle.oamprovider_11.1.1

$ java -jar oamcfgtool.jar app_domain=fs web_domain=OraFusionApp uris_
file=${APPTOP}/fusionapps/applications/atf/security/oam.conf oam_aaa_mode=<'open'
or 'simple'>
```

```
primary_oam_servers=oam_server1 oam_admin_server=http://<OAM ADMINSERVER
HOST>:<OAM ADMINSERVER PORT> oam_version=11 default_authn_scheme=FAAuthScheme
oam_admin_username=<OAM Admin username (the username for the FUSION_APPS_PATCH_
OAM_ADMIN-KEY credential in credstore)> oam_admin_password=<OAM Admin password
(the password for the FUSION_APPS_PATCH_OAM_ADMIN-KEY credential in credstore)>
app_agent_password=<the password for the FUSION_APPS_PATCH_OAM_RWG-KEY credential
in credstore>

$ java -jar oamcfgtool.jar app_domain=crm web_domain=OraFusionApp uris_
file=${APPTOP}/fusionapps/applications/crm/security/oam.conf oam_aaa_mode=<'open'
or 'simple'>
primary_oam_servers=oam_server1 oam_admin_server=http://<OAM ADMINSERVER
HOST>:<OAM ADMINSERVER PORT> oam_version=11 default_authn_scheme=FAAuthScheme
oam_admin_username=<OAM Admin username (the username for the FUSION_APPS_PATCH_
OAM_ADMIN-KEY credential in credstore)> oam_admin_password=<OAM Admin password
(the password for the FUSION_APPS_PATCH_OAM_ADMIN-KEY credential in credstore)>
app_agent_password=<the password for the FUSION_APPS_PATCH_OAM_RWG-KEY credential
in credstore>

$ java -jar oamcfgtool.jar app_domain=fin web_domain=OraFusionApp uris_
file=${APPTOP}/fusionapps/applications/fin/security/oam.conf oam_aaa_mode=<'open'
or 'simple'>
primary_oam_servers=oam_server1 oam_admin_server=http://<OAM ADMINSERVER
HOST>:<OAM ADMINSERVER PORT> oam_version=11 default_authn_scheme=FAAuthScheme
oam_admin_username=<OAM Admin username (the username for the FUSION_APPS_PATCH_
OAM_ADMIN-KEY credential in credstore)> oam_admin_password=<OAM Admin password
(the password for the FUSION_APPS_PATCH_OAM_ADMIN-KEY credential in credstore)>
app_agent_password=<the password for the FUSION_APPS_PATCH_OAM_RWG-KEY credential
in credstore>

$ java -jar oamcfgtool.jar app_domain=fndsetp web_domain=OraFusionApp uris_
file=${APPTOP}/fusionapps/atgpf/atgpf/applications/exploded/oam.conf oam_aaa_
mode=<'open' or 'simple'>
primary_oam_servers=oam_server1 oam_admin_server=http://<OAM ADMINSERVER
HOST>:<OAM ADMINSERVER PORT> oam_version=11 default_authn_scheme=FAAuthScheme
oam_admin_username=<OAM Admin username (the username for the FUSION_APPS_PATCH_
OAM_ADMIN-KEY credential in credstore)> oam_admin_password=<OAM Admin password
 (the password for the FUSION_APPS_PATCH_OAM_ADMIN-KEY credential in credstore)>
app_agent_password=<the password for the FUSION_APPS_PATCH_OAM_RWG-KEY credential
in credstore>

$ java -jar oamcfgtool.jar app_domain=fs web_domain=OraFusionApp uris_
file=${APPTOP}/fusionapps/applications/grc/security/oam.conf oam_aaa_mode=<'open'
or 'simple'>
primary_oam_servers=oam_server1 oam_admin_server=http://<OAM ADMINSERVER
HOST>:<OAM ADMINSERVER PORT> oam_version=11 default_authn_scheme=FAAuthScheme
oam_admin_username=<OAM Admin username (the username for the FUSION_APPS_PATCH_
OAM_ADMIN-KEY credential in credstore)> oam_admin_password=<OAM Admin password
(the password for the FUSION_APPS_PATCH_OAM_ADMIN-KEY credential in credstore)>
app_agent_password=<the password for the FUSION_APPS_PATCH_OAM_RWG-KEY credential
in credstore>

$ java -jar oamcfgtool.jar app_domain=hcm web_domain=OraFusionApp uris_
file=${APPTOP}/fusionapps/applications/hcm/security/oam.conf oam_aaa_mode=<'open'
or 'simple'>
primary_oam_servers=oam_server1 oam_admin_server=http://<OAM ADMINSERVER
HOST>:<OAM ADMINSERVER PORT> oam_version=11 default_authn_scheme=FAAuthScheme
oam_admin_username=<OAM Admin username (the username for the FUSION_APPS_PATCH_
OAM_ADMIN-KEY credential in credstore)> oam_admin_password=<OAM Admin password
 (the password for the FUSION_APPS_PATCH_OAM_ADMIN-KEY credential in credstore)>
```

```
app_agent_password=<the password for the FUSION_APPS_PATCH_OAM_RWG-KEY credential
in credstore>

$ java -jar oamcfgtool.jar app_domain=ic web_domain=OraFusionApp uris_
file=${APPTOP}/fusionapps/applications/ic/security/oam.conf oam_aaa_mode=<'open'
or 'simple'>
primary_oam_servers=oam_server1 oam_admin_server=http://<OAM ADMINSERVER
HOST>:<OAM ADMINSERVER PORT> oam_version=11 default_authn_scheme=FAAuthScheme
oam_admin_username=<OAM Admin username (the username for the FUSION_APPS_PATCH_
OAM_ADMIN-KEY credential in credstore)> oam_admin_password=<OAM Admin password
(the password for the FUSION_APPS_PATCH_OAM_ADMIN-KEY credential in credstore)>
app_agent_password=<the password for the FUSION_APPS_PATCH_OAM_RWG-KEY credential
in credstore>

$ java -jar oamcfgtool.jar app_domain=prc web_domain=OraFusionApp uris_
file=${APPTOP}/fusionapps/applications/prc/security/oam.conf oam_aaa_mode=<'open'
or 'simple'>
primary_oam_servers=oam_server1 oam_admin_server=http://<OAM ADMINSERVER
HOST>:<OAM ADMINSERVER PORT> oam_version=11 default_authn_scheme=FAAuthScheme
oam_admin_username=<OAM Admin username (the username for the FUSION_APPS_PATCH_
OAM_ADMIN-KEY credential in credstore)> oam_admin_password=<OAM Admin password
(the password for the FUSION_APPS_PATCH_OAM_ADMIN-KEY credential in credstore)>
app_agent_password=<the password for the FUSION_APPS_PATCH_OAM_RWG-KEY credential
in credstore>

$ java -jar oamcfgtool.jar app_domain=prj web_domain=OraFusionApp uris_
file=${APPTOP}/fusionapps/applications/prj/security/oam.conf oam_aaa_mode=<'open'
or 'simple'>
primary_oam_servers=oam_server1 oam_admin_server=http://<OAM ADMINSERVER
HOST>:<OAM ADMINSERVER PORT> oam_version=11 default_authn_scheme=FAAuthScheme
oam_admin_username=<OAM Admin username (the username for the FUSION_APPS_PATCH_
OAM_ADMIN-KEY credential in credstore)> oam_admin_password=<OAM Admin password
(the password for the FUSION_APPS_PATCH_OAM_ADMIN-KEY credential in credstore)>
app_agent_password=<the password for the FUSION_APPS_PATCH_OAM_RWG-KEY credential
in credstore>

$ java -jar oamcfgtool.jar app_domain=scm web_domain=OraFusionApp uris_
file=${APPTOP}/fusionapps/applications/scm/security/oam.conf oam_aaa_mode=<'open'
or 'simple'>
primary_oam_servers=oam_server1 oam_admin_server=http://<OAM ADMINSERVER
HOST>:<OAM ADMINSERVER PORT> oam_version=11 default_authn_scheme=FAAuthScheme
oam_admin_username=<OAM Admin username (the username for the FUSION_APPS_PATCH_
OAM_ADMIN-KEY credential in credstore)> oam_admin_password=<OAM Admin password
(the password for the FUSION_APPS_PATCH_OAM_ADMIN-KEY credential in credstore)>
app_agent_password=<the password for the FUSION_APPS_PATCH_OAM_RWG-KEY credential
in credstore>
```

5.5.14 Webcat Patch File Creation Failure

If you apply a RUP that contains BI Publisher artifacts, the BI Presentation servers must not be running. The following error occurs if the BI Presentation servers are running during the deployment of BI Publisher artifacts:

```
java.lang.RuntimeException: Webcat patch file creation failed!
```

To resolve this issue, shut down the BI Presentation servers to release locks on the Oracle BI Presentation Catalog. For more information, see "fastartstop Syntax" in the *Oracle Fusion Applications Administrator's Guide*.

5.5.15 Failure During Deployment of BI Publisher Artifacts

If the deployment of BI Publisher artifacts fails, follow these steps to restore the BI Publisher web catalog and retry the deployment.

1. Click **Cancel** to exit RUP Installer.

   Caution: Do not click **Abort**.

   ---

2. Restore the web catalog from the backup created by RUP Installer. The log file includes a message that provides the location of the backup, for example:

   ```
   Successfully backed up
   "/u01/APPLTOP/instance/BIShared/OracleBIPresentationServicesComponent/coreappli
   cation_obips1/catalog/OracleBIApps" to
   "/u01/APPLTOP/fusionapps/applications/admin/BIP/11.1.3.0.0/en_US/webcat.zip
   ```

3. Restart RUP Installer.

5.5.16 Failures During Starting All Servers

A failure during the **Starting All Servers** configuration task typically happens when one of the servers times out and fails to restart due to resource issues or application specific issues.

5.5.16.1 General Failure

Various platforms and environment configurations can impact how long it will take all servers to actually start during the **Starting All Servers** configuration task. Although RUP Installer waits an average amount of time for this task to complete before it is marked as **Failed**, different platforms may require more time. It is not unusual to receive timeout errors in the log files if the starting of all servers for your environment requires more time than RUP Installer allows. If this task fails, follow these steps:

1. Monitor the status of the servers by reviewing the messages in the server log files or on the console. The log file, *FA_ORACLE_ HOME*/admin/FUSION/log/fapatch/fapatch_ 11.1.3.0.0/StartStop/fastartstop_*timestamp*.log, indicates which server failed to start.

   An example of messages for a server that timed out follow.

   ```
   Time out while performing Start for domain SCMDomain. Waited for 2160 seconds
   [2011-10-21T03:57:52.052--8:00] [fastartstop] [NOTIFICATION:1] [UTIL]
   [oracle.apps.startstop.util.MbeanUtil: runSSCommandOnDomain.868] [tid:37] Start
   operation is completed for domain SCMDomain. Please see SCMDomain.log for
   details.

   [2011-10-21T03:57:52.052--8:00] [fastartstop] [NOTIFICATION:1] [UTIL]
   [oracle.apps.startstop.invoke.StartStopTask: call.221] [tid:37] StartStopTask
   over for domain SCMDomain

   [2011-10-21T03:57:52.052--8:00] [fastartstop] [NOTIFICATION:1] [SST]
   [oracle.apps.startstop.invoke.StartStopTask: call.223] [tid:37] Finished the
   task for the Domain SCMDomain
   ```

2. Review the log files at the domain level to see a summary of the server status for the domain in the previous step: *FA_ORACLE_*

    *HOME/*admin/FUSION/log/fapatch/fapatch_
    11.1.4.0.0/StartStop/*domain name_timestamp*.log.

3. Review the corresponding server logs for the failed servers under the following directory: *APPLICATIONS_CONFIG/*domains/*hostname/domain name/*servers/*server_name/*logs.

4. After you determine and resolve the cause of the failure, return to RUP Installer and click **Retry**.

5. When all servers are up and running, including those that exceeded the timeout limit, click **Abort** in RUP Installer to move to the next configuration task.

5.5.16.2 Failure to Start BIServer

The following exception during the **Starting all Servers** configuration action indicates a failure in starting the BIServer:

```
Start all servers fails to start
Start operation on the component :coreapplication_obips1:, for the instance
:BIInstance: - FAILED
```

The coreapplication_obips1 server log file reports the following error:

```
ecid:]]
[2012-04-10T00:22:20.000-07:00] [OBIPS] [ERROR:16] []
[saw.security.odbcuserpopulationimpl.initialize] [ecid: ] [tid: ] Unable to
create a system user connection to BI Server during start up. Trying again.[[
File:odbcuserpoploaderimpl.cpp
Line:325
Location:
saw.security.odbcuserpopulationimpl.initialize
saw.catalog.local.loadCatalog
saw.subsystems.catalogbootstrapper.loadcatalog
saw.webextensionbase.init
saw.sawserver
ecid:]]
[2012-04-10T00:22:25.000-07:00] [OBIPS] [NOTIFICATION:1] [] [saw.sawserver]
[ecid: ] [tid: ] Oracle BI Presentation Services are shutting down.[[
File:sawserver.cpp
Line:706
Location:
saw.sawserver
ecid:
```

Perform the following steps to work around this issue.

1. Select **Retry**, which shuts down and starts bi_server1.

2. Monitor the fastartstop log files and the state of bi_server1(BIDomain).

3. As soon as bi_server1 restarts, as indicated by a RUNNING status, start the component coreapplication_obiccs1 or all the components of type OracleBIClusterControllerComponent using opmnctl.

    Example syntax follows:

```
*/BIInstance/bin/opmnctl startproc ias-component=coreapplication_obiccs1
```

5.5.17 Failure During IPM Import

If the configuration task for importing IPM artifacts fails with the following error, follow the instructions in Step 7 in Section 4.12.1, "Prerequisites for the Deployment of IPM Artifacts". Then run the following command:

```
importIPMApplication() & importIPMInput() WLST commands have not run
successfully
```

5.5.18 Merging SOA Composite JDeveloper Customizations While Installing a RUP

If you performed JDeveloper customizations to a SOA composite and you deployed the composite to the SOA runtime, RUP Installer reports an error during **Online Preverification**, which instructs you to take the newer version of the composite that is in the RUP. You must then merge your customizations by performing the following steps.

1. If any customizations are detected, the **Online Preverification** results display the SOA composite name, its location in the *FA_ORACLE_HOME/stripe/*`deploy` directory, and the requirement for you to merge JDeveloper customizations into the sca_*.jar file in *FA_ORACLE_HOME* before proceeding with RUP Installer. The *stripe* in the directory path refers to crm, hcm, fscm, and so on.

2. Open the custom SOA workspace and the customized version of the Fusion Applications SOA composite in JDeveloper using "Oracle Fusion Applications Developer". For more information, see "Customizing SOA Composites with JDeveloper" in the *Oracle Fusion Applications Web User Interface Developer's Guide for Oracle Application Development Framework*.

3. Import the composite `sca_*.jar` file from *FA_ORACLE_HOME/stripe/*`deploy` into the project, for example revision 11.1.3.0.0, in JDeveloper. Make note of this revision number in the deployment window because you will need it in Step 8.

4. Restart JDeveloper in the Oracle Fusion Applications Administrator Customization role.

5. Verify that there are no errors in JDeveloper.

6. Verify that the changes introduced in both the customized version and the patched version are present.

7. Right-click the composite project in the Application Navigator, select **Deploy**, select the composite, click **Deploy to SAR**, and click **Next**.

8. Manually change the value in **New Revision ID** to the revision from Step 3, for example, 11.1.3.0.0, and click **Finish**.

9. If the deployment folder is set to a location different from that of the *FA_ORACLE_HOME/stripe/*`deploy` directory, copy and replace the JAR in the location mentioned in the error message of this SOA Composite. If your file name is different, rename it to the original name. You must copy the jar file in the correct format to *FA_ORACLE_HOME/stripe/*`deploy`. For example if you have `sca_ContractsDeliverablePurchaseDocAttrReadComposite_rev11.1.2.0.0.jar` in JDeveloper, then you must copy it back to *FA_ORACLE_HOME/stripe/*`deploy` as `sca_ContractsDeliverablePurchaseDocAttrReadComposite.jar`.

10. To proceed with the installation of the RUP, select **Retry**.

For more information about customizing SOA composites, see "Customizing and Extending SOA Components" in the *Oracle Fusion Applications Extensibility Guide*.

5.5.19 Troubleshooting SOA Composite Deployment Failures

This section describes how to recover from out-of-memory errors during the **Deploying SOA Composites** configuration task. The following topics are described:

- SOA Composite Log Files
- Composite Revision is Already Deployed
- Cannot Set Default Composite

5.5.19.1 SOA Composite Log Files

The following log files are generated by the deployment of SOA composites:

- Client side log files where individual domain logs reside: *FA_ORACLE_ HOME*/admin/FUSION/log/fapatch/fapatch_11.1.3.0.0/soalogs

- Log files for the failed domain:

  - *APPLICATIONS_CONFIG*/domains/*hostname/domain name*/servers/*server name*/logs/soa_server1.log

  - *APPLICATIONS_CONFIG*/domains/*hostname/domain name/*servers/*server name/*logs/soa_server1.out

  - *APPLICATIONS_CONFIG*/domains/*hostname/domain name*/servers/*server name*/logs/soa_server1-diagnostic.log

  - *APPLICATIONS_CONFIG*/domains/*hostname/domain name/*servers/*server name/*logs/AdminServer.log

5.5.19.2 Composite Revision is Already Deployed

Normally, a failed SOA composite is undeployed by RUP Installer. However, if the failure of the deployment is due to SOA servers running out of memory, then RUP installer cannot recover. As a result, a failure message such as, CFGEX-00062: Composite revision "default/composite name!11.1.3.0.0" is already deployed, may occur.

An example of a complete error message follows:

```
[2011-12-30T04:24:38.613-08:00] [apps]
[ERROR] [] [oracle.apps.CRMDomain] [tid: 58]
[ecid: 0000JIEvTHGEGR9ZvdYBV11EzMvF00000c,0]
CFGEX-00073 : SOA composite "/u01/APPLICATIONS_
BASE/fusionapps/applications/crm/deploy/sca_
ContractsTermLibTemplatesComposite.jar"
deployment failed for Domain "CRMDomain".[[
Action : See logs for details. oracle.as.install.
fapatchconfig.exception.PatchsetConfigException:
CFGEX-00073 : SOA composite "/u01/APPLICATIONS_BASE/fusionapps/applications/
crm/deploy/sca_ContractsTermLibTemplatesComposite.jar" deployment failed for
Domain "CRMDomain".
      ….
Caused by: oracle.as.install.fapatchconfig.exception.PatchsetConfigException:
CFGEX-00062 : Composite revision "default/
ContractsTermLibTemplatesComposite!11.1.3.0.0" is already deployed.
```

To resolve this issue, you must manually undeploy the composite.

> **Note:** Ensure that you undeploy only the revision deployed by RUP
> Installer. Do not undeploy the previous version.

To undeploy, use WebLogic Server Tool (WLST) commands or the Fusion Applications
Control console.

5.5.19.2.1 Undeploy SOA Composites Using WLST Commands Follow these steps to
undeploy the composite using WLST commands:

1. Start WLST:

   ```
   (Unix) APPLICATIONS_BASE/soa/common/bin/wlst.sh
   ```

   ```
   (Windows) APPLICATIONS_BASE\soa\common\bin\wlst.cmd
   ```

2. Run the `sca_undeployComposite` command using the following syntax:

   ```
   sca_undeployComposite(serverURL, compositeName,
   revision, [user], [password], [partition])
   ```

   where the variables have values as follows:

   - `serverURL` contains the host and port of the SOA cluster Managed Server of
     the domain that the SOA composite failed to deploy

   - `compositeName` is the name of the composite to be undeployed

   - `revision`, in the case of Release 2 Update 1 (11.1.3.0.0), should be 11.1.3.0.0
     by default.

   Example:

   ```
   wls:/mydomain/ServerConfig>  sca_undeployComposite
   ("http://myhost10:7001",
   " ContractsDeliverablePurchaseAgrmntFlowComposite ", "11.1.3.0.0")
   ```

   You are prompted for user name and password to execute the command.

   For more information, see "Oracle SOA Suite Custom WLST Commands" in the
   Oracle Fusion Middleware WebLogic Scripting Tool Command Reference.

5.5.19.2.2 Undeploy SOA Composites Using the Fusion Applications Control Console Follow
these steps to undeploy the composite using the Fusion Applications Control console:

1. In the Fusion Applications Control console, connect to the domain where the SOA
   composite failed to deploy.

2. Navigate to Farm_*Domain*->soa-infra->default.

3. Locate the composite and revision, such as 11.1.3.0.0 as shown in this example:

   ```
   ContractsDeliverablePurchaseAgrmntFlowComposite [11.1.3.0.0]
   ```

4. Right click on the composite and select **SOA deployment** > **Undeploy**.

5.5.19.3 Cannot Set Default Composite

You may receive the following error during the deployment of a SOA composite. For
this example, the `HcmEmploymentProcessesChngWkHrsComposite` composite is
shown:

```
Step FIND_BASE_COMPOSITE:Find the base composite for patch. It will be
```

```
current default composite of the series
  ==> failed: Error in getting default
composite:default/HcmEmploymentProcessesChngWkHrsComposite, The configuration
file, deployed-composites.xml, does not contain the
default/HcmEmploymentProcessesChngWkHrsComposite composite-series element.
```

To resolve this issue, manually deploy the missing composite by executing the following commands on a Windows platform:

```
SET JAVA_HOME=REPOSITORY_LOCATION\jdk6
REPOSITORY_LOCATION\provisioning\ant\bin\ant -f
APPLICATIONS_BASE/fusionapps/soa/bin/ant-sca-deploy.xml -DsarLocation
APPLICATIONS_BASE/fusionapps/applications\hcm/deploy\sca_
HcmEmploymentProcessesChngWkHrsComposite.jar
-DserverURL http://my_host:9420 -Duser
FUSION_APPS_PROV_PATCH_APPID -Dstdinpassword true -Doverwrite true
-DfailOnError true deploy
```

5.5.20 Failure During Applying BI Metadata Updates

If a failure occurs during the **Apply BI Metadata Updates** task due to conflicts, you must resolve the conflicts before the task can proceed. You must resolve the conflicts as soon as the task fails and then select **Retry** to allow RUP Installer to proceed.

To get information about conflicts, review the related report at this location:

```
FA_ORACLE_HOME/fusionapps/bi/.biapps_patch_
storage/update/timestamp/update-report-timestamp.txt
```

Refer to the following types of conflicts for information about how to resolve them.

1. To resolve Oracle BI RPD conflicts, use the decision file located at *FA_ORACLE_HOME/*`fusionapps/bi/.biapps_patch_`
    `storage/update/`*timestamp/*`patchrpd_decision_file.csv`. The decision file lists the decisions that would have been displayed in the Define Merge Strategy screen of the Merge Wizard if the merge had been performed in the Oracle BI Administration Tool. The decision file provides a record of all items that can be affected by user input.

    a. Use the **Load Decision File** button in the **Define Merge Strategy** screen of the Merge Wizard to load the merge decisions, and then change the decisions if needed. In the decision window, ensure you select **Current**, as those are Oracle's changes. You can then complete the merge in the Oracle BI Administration Tool.

    b. Use Enterprise Manager to upload the merged RPD. For more information, see "Using Fusion Middleware Control to Upload a Repository and Set the Oracle BI Presentation Catalog Location" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*.

    c. Return to RUP Installer and select **Retry**.

    For more information, see "Resolving Conflicts for Oracle BI Repository (RPD) Updates"' in the *Oracle Fusion Middleware Reference Guide for Oracle Business Intelligence Applications* and

2. If you made customizations to the content of the Oracle BI Presentation Catalog, conflicts may arise when the Oracle BI Presentation Catalog is updated by RUP Installer. You must resolve these conflicts and then run the BI Metadata Update

Tool (MUT) which was run by RUP installer. The patch log file lists the conflicts and the location of the runtime and Oracle home Presentation Catalogs.

Follow the steps below to resolve Oracle BI Presentation Catalog conflicts:

a. Back up the runtime Oracle BI Presentation Catalog. This is the customized Oracle BI Presentation Catalog you were using before running RUP Installer.

b. Start the Catalog Manager and open the runtime Oracle BI Presentation Catalog in offline mode.

c. Start another instance of the Catalog Manager, and open the Oracle home Oracle BI Presentation Catalog in offline mode. This Oracle BI Presentation Catalog contains the content last delivered by Oracle.

d. Review the list of conflicts in the patch log file.

e. Archive the runtime Oracle BI Presentation Catalog. For instructions on archiving a Oracle BI Presentation Catalog, see "Archiving and Unarchiving Using Catalog Manager" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*.

f. For each object with a conflict, copy the object in the Oracle home Presentation Catalog and paste it into the runtime Presentation Catalog, using the Force paste option. For instructions on copying and pasting objects, see "Copying and Pasting Objects" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*.

g. Rerun the BI Metadata Update Tool (MUT). RUP Installer runs the MUT and the last part of the MUT generates a log file that contains the exact command to use for rerunning MUT.

For more information, see "Resolving Conflicts for Oracle BI Presentation Catalog Updates" in the *Oracle Fusion Middleware Reference Guide for Oracle Business Intelligence Applications.*

3. To resolve JAZN policy store conflicts, see "Resolving Patch Differences" in the *Oracle Fusion Middleware Oracle Authorization Policy Manager Administrator's Guide (Oracle Fusion Applications Edition)*. Also see "Upgrading Oracle Fusion Applications Policies" in the *Oracle Fusion Middleware Oracle Authorization Policy Manager Administrator's Guide (Oracle Fusion Applications Edition)* for background information.

5.5.21 AttachHome Script Hangs

If the `attachHome` script hangs, when following the steps in Section 5.2.11, "Confirm All Oracle Homes Are Registered in the Central Inventory", run `attachHome` with the following additional arguments: `-waitforcompletion -nowait`.

5.5.22 The runInstaller.sh -updateHomeDeps Command Hangs

If the `runInstaller -updateHomeDeps` command hangs, when following the steps in Section 5.2.11, "Confirm All Oracle Homes Are Registered in the Central Inventory", run this command with the following additional arguments: `-waitforcompletion -nowait`.

5.5.23 Verify Your Installation

Perform the steps in "Verifying Installation" in the *Oracle Fusion Applications Post-Installation Guide*.

6

Maintaining Oracle Fusion Applications Languages

This chapter describes how to install and maintain a set of languages in Oracle Fusion Applications.

This chapter contains the following topics:

- Introduction to Language Maintenance in Oracle Fusion Applications
- Prepare to Install a Language Pack Pre-Down Time
- Prepare to Install a Language Pack - During Down Time
- Install a Language Pack
- Troubleshooting Language Pack Installer Sessions
- Maintaining Languages

6.1 Introduction to Language Maintenance in Oracle Fusion Applications

Oracle Provisioning and RUP Installer install and upgrade only the English language. To add a language or upgrade an existing language, use Language Pack Installer. If patches containing translatable artifacts were previously applied to this environment, you apply the translated versions of each of those patches after you install the new language.

This section provides an introduction to the following concepts related to language packs:

- Language Packs
- Language Pack Installer
- Language in the Policy Store
- Artifacts Supported by Language Pack Installer
- Language Pack Installer Configuration Tasks

6.1.1 Language Packs

A language pack for a given language and release contains artifacts at the specific release level that are translated to the specific language. Translated artifacts include Oracle Fusion Applications seed data that is uploaded into Oracle Fusion Applications database, SOA resource bundles, JEE resource bundles, and Applications Policies. You install language packs with Language Pack Installer.

6.1.2 Language Pack Installer

Language Pack Installer enables you to add a language to your Oracle Fusion Applications environment and delivers translated artifacts for that language. You run Language Pack Installer in interactive mode and proceed through the installation by providing information in the user interface when prompted. For more information, see Section 5.1.3, "RUP Installer User Interface", which is the same as the Language Pack Installer user interface.

Language Pack Installer performs the following tasks:

- Copies language artifacts to the appropriate directory in *FA_ORACLE_HOME*. For more information, see Section 2.1.2, "Oracle Fusion Applications Oracle Home".

- Enables the new language in the FND_LANGUAGES table.

- Runs the AD Administration process to maintain multi-lingual tables, which prepares the tables for the data to be copied from the source language to the new language.

- Updates the language content using the database artifacts for the new language that are included in the language pack.

- Applies the updated translated middleware database content.

- Deploys Service-Oriented Architecture (SOA) resource bundles.

- Uploads LDIF translation XLF files to Oracle Internet Directory (OID).

- Enables the language.

6.1.3 Language in the Policy Store

The policy store maintains attributes in only one language. If you want to override the base English strings in the policy store, you set the -J-DupdateJAZNPolicyStore (-DupdateJAZNPolicyStore for Windows) option to true when you install the Language Pack. The Description and Displayname are the two attributes which are translatable and are loaded in JAZN files in the Language Pack.

6.1.4 Artifacts Supported by Language Pack Installer

Language Pack Installer supports the installation and automated deployment of most middleware and database artifacts used by Oracle Fusion Applications that are related to languages. Depending on the type of artifact included in the Language Pack, the artifact deployment may require manual actions. For more information about manual deployment of these artifacts, see Chapter 4, "Patching Oracle Fusion Applications Artifacts".

Table 6–1 provides a quick reference that depicts how Language Pack Installer supports the Oracle Fusion Applications artifacts that could be included in a Language Pack.

An explanation of the information presented in this table follows:

- Automated Actions Performed by Language Pack Installer

  Language Pack Installer always copies the artifacts from the Language Pack to the appropriate location on your system. This column describes additional actions that are performed automatically for each artifact.

- Actions to Be Performed Manually

This column describes the actions you must perform when the Language Pack includes the specified artifact.

Table 6–1   Artifacts Supported by Language Pack Installer

Artifact Type	Automated Actions Performed By Language Pack Installer	Actions To Be Performed Manually
Translated ADF resource bundles	Deploy resource bundles.	None.
Applications Policies (system-jazn-data .xml)	Deploy changes to the policy store. Also updates the policy store if you chose to override the base English strings in the policy store.	Back up the policy store before installation and choose the deployment method during configuration.
Oracle Business Intelligence Publisher (Reports and Captions)	Deploy to the Business Intelligence repository using Catalog Manager, and start the BI Presentation server after patching.	None.
Common Resource (Activity Strings)	None.	None.
Flexfields	Deploy flexfields.	None.
LDAP Data (LDIF)	Upload translated LDIF content to the identity store.	None.
Translated content for seed data (XLF)	Upload translated seed data.	None.
SOA Resource Bundle	Deploy SOA resource bundle and restart dependent composites.	None.

6.1.5 Language Pack Installer Configuration Tasks

During the installation phase, Language Pack Installer copies all files from the Language Pack to Oracle Fusion Applications Oracle home. After the file copy is completed, Language Pack Installer starts the Policy Store Analysis, as described in Table 6–5. Then Language Pack Installer calls Configuration Assistants to perform the remaining tasks required to update and deploy the artifacts included in the Language Pack. If any tasks fail during the configuration phase, you can abort or retry the task. For more information, see Section 5.5.3, "General Troubleshooting During the Configuration Phase".

Table 6–2 provides a list of possible configuration tasks, including steps within the tasks. The Retry Behavior column describes what Language Pack Installer does after a configuration task fails and you select the **Retry** button. If available, links are provided to relevant troubleshooting sections.

Table 6–2   Configuration Tasks Run by Language Pack Installer

Name	Mandatory	Description	Retry Behavior
Activate Language	Yes	Activates the language in the database and runs the Maintain Multilingual Tables utility to maintain the tables related to the newly activated language. For more information, see Section 10.3.4, "Maintaining Multi-lingual Tables".	Runs Activate Language again.

Table 6–2   (Cont.) Configuration Tasks Run by Language Pack Installer

Name	Mandatory	Description	Retry Behavior
Offline Preverification	Yes	Performs the following validation checks while all servers are shutdown: ■ Policy Store ■ Database Content Upload	Runs failed steps.
Synchronize Multilingual Tables	Yes	Prepares tables for the data to be copied from the source language to the new language.	Restart from failure.
Apply Middleware Language Patches	Yes	Applies both the patches in the Language Pack repository and the downloaded patches from My Oracle Support in the `post_repo_patches` directory.	Applies the failed patches. See Section 5.5.7, "Troubleshooting Applying Middleware Patches".
Load Database Components	Yes	Uploads the database content packaged in the Language Pack to the database.	Runs failed database commands. See Section 5.5.10, "Troubleshooting Loading Database Components".
Deploy Applications Policies (jazn-data.xml)	Yes	Oracle Fusion Applications allows one policy store per language. The `jazn-data.xml` files in the Language Pack are processed only if you choose to change the policy store language to be the same as that of the Language Pack being installed. Otherwise, this step does not run.	Deploys the failed stripes. See Section 5.5.12, "Troubleshooting Deployment of Applications Policies".
Deploy BI Publisher Artifacts	Yes	Copies captions and deploys BI Presentation Catalog to the Oracle Business Intelligence repository using Catalog Manager.	Starts from the beginning of the task. See Section 5.5.14, "Webcat Patch File Creation Failure".
Verify Node Manager and OPMN Status	Yes	Checks for access to the Node Manager and the Oracle Process Manager and Notification Server (OPMN) control process. You must not exit out of Language Pack Installer during this task.	This step will only fail if the node manager and OPMN control processes are already running. In case it fails, restart the Node Manager and OPMN and click **Retry**.
Start All Servers	No	Starts servers that must be running for the deployment of the remaining artifacts in the Language Pack.	Restarts failed servers. See Section 5.5.16, "Failures During Starting All Servers".
Online Preverification	Yes	Performs validation checks that require all servers to be running. The following validation steps are performed during this task: ■ Flexfields ■ LDAP Data (LDIF) ■ SOA Resource Bundles	Runs failed steps. See Section 5.5.9, "EditTimedOutException Error During Online Preverification".

Table 6–2 (Cont.) Configuration Tasks Run by Language Pack Installer

Name	Mandatory	Description	Retry Behavior
Deploy Flexfields	No	Deploys flexfields to the domain that hosts the `FndSetup` application.	Starts from the beginning of the task.
Deploy LDAP Data (LDIF)	No	Uploads LDIF XLIFF translations to identity store.	Retries only failed XLIFF files.
Deploy SOA Resource Bundles	Yes	Deploys SOA Resource Bundles to the corresponding SOA servers.	Deploys failed SOA resource bundles.
Restart All SOA Servers	No	Restarts all SOA servers in the environment.	Starts at the beginning of the task.

6.2 Prepare to Install a Language Pack Pre-Down Time

This section describes the following preparation steps for installing a language pack, all of which can be performed before your scheduled down time.

- Download the Language Pack Repository
- Confirm Oracle Fusion Applications Installation is Complete
- Verify Your OPatch Version
- Confirm Memory Settings
- Confirm Host Name (Unix)
- Confirm the Local Port Range Value
- Confirm Database Settings
- Confirm All Oracle Homes Are Registered in the Central Inventory
- Maintain Versions of Customized BI Publisher Reports

6.2.1 Download the Language Pack Repository

The language pack repository contains the language pack installer, translated Oracle Fusion Middleware patches, and the Oracle Fusion Applications language pack that are required to install a language pack for a specific language in an existing Oracle Fusion Applications environment. You download the repository from the Oracle Fusion Applications Product Media Package to a location of your choice. This directory is referred to as *REPOSITORY_LOCATION*.

6.2.1.1 Obtaining the Software

Oracle groups its software releases by product area. A **Product Media Pack** refers to those groupings. Each media pack may also include a zipped file containing electronic documentation files or "Quick Install" files, which facilitate the initial installation of the software.

Once you have completed the software licensing agreements, you can obtain the Oracle Fusion Applications software using one of these two methods:

- **Oracle Software Delivery Cloud Portal**: Provides you with a readme document that helps you to determine which media you need to fulfill the license you have purchased. You download only the media you need. This is the default delivery method.

■ **Oracle Store**: Provides a complete set of the software in DVD format. You use only the DVDs covered by your software licensing agreement.

Using either method, you can obtain the Oracle Fusion Applications language pack repository.

6.2.1.2 Downloading from the Oracle Software Delivery Cloud Portal

Go to http://edelivery.oracle.com/ and follow these instructions:

1. Complete the Export Validation process by entering basic identification information using the online form.

2. On the Media Pack Search page, specify the product pack and platform to identify the media pack you want to download. If you do not know the name of the product pack, you can search for it using the license list.

3. Choose the appropriate media pack from the search results and download the language pack repository (in zipped format). You can download the repository to a location of your choice.

4. Extract the contents of all zipped files to the same target directory. The directory must be on a networked drive or shared disk so that it will be accessible to all the hosts in your new environment. The installers are normally located in the `installers` subdirectory under `REPOSITORY_LOCATION`.

> **Note:** You should avoid creating the repository in a deeply nested directory on Windows. The Windows PATH variable has a limited size, and long directory names may cause it to overflow. For example, `c:\work\my_repository` is a better choice than `c:\Work\WorkInProgress\FusionApps\FusionAppsv1\Nov2011\tempfiles\my_repository`.

6.2.1.3 Language Pack Installer

Table 6–3 list the installers in the language pack repository.

Table 6–3   Language Pack Installers

Media Label Name	Staging Destination
Language Pack Installer	(Unix) `REPOSITORY_LOCATION/language_code/installers/fusionapps/Disk1/runInstaller`
	(Windows) `REPOSITORY_LOCATION\language_code\installers\fusionapps\Disk1\Setup.exe`
	or `REPOSITORY_LOCATION\language_code\installers\fusionapps\Disk1\install\Win64\Setup.exe`

6.2.2 Confirm Oracle Fusion Applications Installation is Complete

If you are installing a language pack on a freshly installed Oracle Fusion Applications environment, ensure that you have performed all tasks described in "Postinstallation Tasks" in the *Oracle Fusion Applications Installation Guide.*

If you are installing a language pack on a upgraded environment, ensure that you have followed all tasks described in Section 5.4.2, "Complete the Post Installation Tasks".

In either case, you must also perform the steps in the "Post-Installation" section of Oracle Fusion Applications release notes.

6.2.3 Verify Your OPatch Version

Follow this step only if you have updated OPatch in the *FA_ORACLE_HOME* outside of what Oracle Provisioning and RUP Installer installs.

Oracle Fusion Applications is compatible with a specific version of OPatch instead of the generic version of OPatch. If an incompatible version of OPatch exists in *FA_ORACLE_HOME*, errors can occur while applying patches and running Language Pack Installer. The compatible version of OPatch is available on My Oracle Support under patch 14044793.

If the file, *FA_ORACLE_HOME/*`OPatch/ocm/lib/emocmclnt.jar` exists, then you have an incompatible version of OPatch, and you must contact Oracle Support to fix this issue. On Windows, look for *FA_ORACLE_HOME*`\OPatch\ocm\lib\emocmclnt.jar`.

6.2.4 Confirm Memory Settings

Confirm that memory requirements are met on the primordial host that the Language Pack installer is launched from. The primordial host is where the Administration Server for the Common Domain runs.

Language Pack Installer requires at least 6GB of free RAM on the 64-bit domains to be up during the installation. Language Pack installer also requires at least 6GB of free RAM on the 64-bit primordial host that the installer is launched from, for the duration of the Language Pack installation. This 6GB of free memory requirement is in addition to the memory requirement for all servers, including the Administration Servers on the primordial host that is already up and running. Oracle also recommends at least 1GB of additional free memory on the primordial host during the Language Pack installation as a safety net.

For example, if the BI domain is provisioned on the primordial host, then Language Pack Installer requires this 64-bit primordial host to have a minimum of 12GB of RAM. If you have two 64-bit hosts with the BI domain provisioned on a different host from the primordial host, then one host runs the Administration Server and the BI servers, while the other host runs Language Pack Installer, which requires a connection to the Administration Server that is running. If you run Language Pack installer and the Administration Server on the same primordial host with insufficient memory, then the Administration Server and Managed Servers may fail.

6.2.5 Confirm Host Name (Unix)

For Unix platforms, confirm that the host names are correctly formatted in the `/etc/hosts` file, and that this file contains entries for all hosts used by Oracle Fusion Applications to ensure that all hosts are visible from the primordial host. The `/etc/hosts` file is a network configuration file that associates IP addresses with host names and host alias names, if used. Every hosts file in Unix platforms should have an entry for the IP address `127.0.0.1`, with the name `localhost` following it. For more information, see "Edit Host Names (Linux)" in the *Oracle Fusion Applications Installation Guide*.)

6.2.6 Confirm the Local Port Range Value

Check the local port range value in `/proc/sys/net/ipv4/ip_local_port_` `range` before starting the Language Pack installation. The recommended value is `32768 61000`. If the range is set to any value below `32768`, a system process could potentially use a port that was assigned to one of the Managed Servers.

To set the correct local port range, log in as the root user and run the following command:

```
echo "32768 61000" > /proc/sys/net/ipv4/ip_local_port_range
```

6.2.7 Confirm Database Settings

Review the following steps to confirm that your database settings are optimized for the language pack installation.

1. Refer to Oracle Fusion Applications release notes for information about database tuning parameters, to avoid time out conditions during the installation.

2. Confirm that the open file limit is set properly.

   Language Pack Installer uses multiple workers for uploading database content. The number of workers used dictates the open file limit setting for the machine where you run the Language Pack Installer. To understand how the number of the workers are calculated and the open file limit setting that is required for the workers, see Section 3.1.2.1, "Worker Processes". For more information, see "Increase the Open Files Limit" in the *Oracle Fusion Applications Installation Guide*.

3. Confirm that the SQL*Net Timeout Configuration is set properly.

   The exact setting in your environment depends on your network configuration and machine resources. Refer to "SQLNET.EXPIRE_TIME Parameter" and "INBOUND_CONNECT_TIMEOUT Parameter" in the *Oracle Fusion Applications Performance and Tuning Guide* to determine the parameters that need to be set.

6.2.8 Confirm All Oracle Homes Are Registered in the Central Inventory

Oracle Provisioning records information about the following Oracle homes separately from information about other products: Oracle Business Intelligence (Oracle BI), Oracle Global Order Promising (GOP), Web tier, and Web tier Common Oracle home installation information. Patching expects information about all products to be recorded in the same place. To transfer information about the BI, GOP, and Web tier installations to the same location as information about other products, perform the following steps. For more information about home directories, see "Provisioned Oracle Fusion Applications Home Directories" in the *Oracle Fusion Applications Administrator's Guide*.

1. Verify that the default Inventory Pointer file points to the central inventory on the primordial host on which Language Pack Installer runs. The default Inventory Pointer is in the following locations:

   - Unix: /etc/oraInst.loc

   - Solaris: `/var/opt/oracle/oraInst.loc`

   - Windows: located in the registry key, `\\HKEY_LOCAL_` `MACHINE\\Software\Oracle\inst_loc`

2. Run `attachHome` from the BI Oracle home, for example, *APPLICATIONS_* *BASE*`/fusionapps/bi`.

```
(Unix) BI_HOME/oui/bin/attachHome.sh -jreLoc JAVA_HOME_LOCATION
(Windows) BI_HOME\oui\bin\attachHome.cmd -jreLoc JAVA_HOME_LOCATION
```

3. Run `attachHome` from the GOP Oracle home, for example, *APPLICATIONS_BASE*/fusionapps/gop.

```
(Unix) GOP_HOME/oui/bin/attachHome.sh -jreLoc JAVA_HOME_LOCATION
(Windows) GOP_HOME\oui\bin\attachHome.cmd -jreLoc JAVA_HOME_LOCATION
```

4. Run `attachHome` from the Web tier Oracle home, for example, *APPLICATIONS_BASE*/webtier_mwhome/webtier.

```
(Unix) WEBTIER_HOME/oui/bin/attachHome.sh -jreLoc JAVA_HOME_LOCATION
(Windows) WEBTIER_HOME\oui\bin\attachHome.cmd -jreLoc JAVA_HOME_LOCATION
```

5. Run `attachHome` from the Web tier Common Oracle home, for example, *APPLICATIONS_BASE*/webtier_mwhome/oracle_common.

```
(Unix) WEBTIER_COMMON_HOME/oui/bin/attachHome.sh -jreLoc JAVA_HOME_LOCATION
(Windows) WEBTIER_COMMON_HOME\oui\bin\attachHome.cmd -jreLoc JAVA_HOME_LOCATION
```

6. Register the dependency between the BI Oracle home and Oracle Common Oracle home.

   Run Oracle Universal Installer with the `-updateHomeDeps` option and pass a dependency list. The syntax for the dependency list is:

   ```
   HOME_DEPENDENCY_LIST={ORACLE_HOME:DEPENDENT_ORACLE_HOME}
   ```

   Example for Business Intelligence:

   ```
   (Unix) BI_HOME/oui/bin/runInstaller -updateHomeDeps "HOME_DEPENDENCY_LIST=
   {APPLICATIONS_BASE/fusionapps/bi:APPLICATIONS_BASE/fusionapps/oracle_common}"
   -jreLoc JAVA_HOME_LOCATION

   (Windows) BI_HOME\oui\bin\setup.exe -updateHomeDeps "HOME_DEPENDENCY_LIST=
   {APPLICATIONS_BASE\fusionapps\bi:APPLICATIONS_BASE\fusionapps\oracle_common}"
   -jreLoc JAVA_HOME_LOCATION
   ```

7. Register the dependency between Web tier Oracle home and Web tier Common Oracle home.

   ```
   (Unix) WEBTIER_HOME/oui/bin/runInstaller -updateHomeDeps "HOME_DEPENDENCY_LIST=
   {APPLICATIONS_BASE/webtier_mwhome/webtier:APPLICATIONS_BASE/webtier_
   mwhome/oracle_common}"
   -jreLoc JAVA_HOME_LOCATION

   (Windows) WEBTIER_HOME\oui\bin\setup.exe -updateHomeDeps "HOME_DEPENDENCY_LIST=
   {APPLICATIONS_BASE\webtier_mwhome\webtier:APPLICATIONS_BASE\webtier_
   mwhome\oracle_common}"
   -jreLoc JAVA_HOME_LOCATION
   ```

8. Verify that the central inventory now contains the correct GOP, BI, and Web tier information. Open the `inventory.xml` file from the `ContentsXML` subdirectory in your central inventory directory using a text editor. You can find your central inventory directory by looking in the default Oracle Inventory pointer file mentioned in Step 1. Verify that there are entries for GOP and for BI, and that the BI entry lists the Oracle Common dependency you specified in Step 6. Do the same for Web tier information. Ensure that you do not modify `inventory.xml` in any way, as this may corrupt your system.

   Example entries in inventory.xml:

```
<HOME NAME="OH1109401105" LOC="APPLICATIONS_BASE/fusionapps/gop" TYPE="O"
IDX="11">
<HOME NAME="OH198367808" LOC="APPLICATIONS_BASE/fusionapps/bi" TYPE="O"
IDX="12">
   <DEPHOMELIST>
      <DEPHOME LOC="APPLICATIONS_BASE/fusionapps/oracle_common"/>
   </DEPHOMELIST>
</HOME>
<HOME NAME="OH987588708" LOC="APPLICATIONS_BASE/webtier_mwhome/webtier"
TYPE="O" IDX="13">
   <DEPHOMELIST>
      <DEPHOME LOC="APPLICATIONS_BASE/webtier_mwhome/oracle_common"/>
   </DEPHOMELIST>
</HOME>
<HOME NAME="OH1271096710" LOC="APPLICATIONS_BASE/webtier_mwhome/oracle_common"
TYPE="O" IDX="14">
   <REFHOMELIST>
      <REFHOME LOC="APPLICATIONS_BASE/webtier_mwhome/webtier"/>
   </REFHOMELIST>
</HOME>
```

> **Note:**   Rerunning the ATTACH_HOME command does not cause any issues.

6.2.9 Maintain Versions of Customized BI Publisher Reports

Ensure that you have your own versions of any customized BI Publisher reports. If a Language Pack includes an update to a catalog object that was delivered with an Oracle Fusion application, the patch will overwrite any customizations applied to the original report. For more information, see "Before You Begin Customizing Reports" in the *Oracle Fusion Applications Extensibility Guide*.

6.3 Prepare to Install a Language Pack - During Down Time

The section describes the following mandatory preparation steps for installing a language pack, all of which must be performed during your system down time.

- Verify the Status of Servers and Processes

- Perform Required Backups

- Apply Mandatory Prerequisite Patches

6.3.1 Verify the Status of Servers and Processes

This section contains steps to follow for all platforms. For Windows platforms, also follow the steps in Section 6.3.1.8, "Steps For Windows Platforms"

6.3.1.1 Stop Servers

Stop only Fusion Applications middle tier servers and processes including BI servers and WLS administration and managed servers.

6.3.1.2 Confirm the OPMN Control Process and Node Manager Are Running

Confirm that the OPMN control process and Node Manager are running. If they are not running, follow the steps in Table 5–4 under "Configuration Progress (continued)" to start them.

6.3.1.3 Start the OPSS Security Store

Start the OPSS Security Store if it is not already running. For more information, see "Starting and Stopping Oracle Internet Directory" in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management (Oracle Fusion Applications Edition)*. If this server is not running prior to starting the installation, the related configuration tasks will fail. For more information, see Section 5.5.11, "LdapServerCheck Failure".

6.3.1.4 Confirm The Database Is Running And In An Idle State

Confirm that there are no active jobs or processes running against the database. If there are, stop all background jobs, including jobs in the database and active processes. If you stop all servers, including ESS servers, most Oracle Fusion Applications processes are shut down. However, some database jobs could still be running or scheduled to start. These processes must be stopped so that they do not start while patching is in progress. Stop all background jobs, including jobs in the database and active processes.

To confirm if the database is running in idle mode, you can follow the steps below:

1. Start SQL*Plus and connect as the SYS user and run the following SQL*Plus queries.

2. To retrieve a list of active SQL processes:

   ```
   select a.sid, a.serial#, b.sql_text
   from v$session a, v$sqlarea b
   where a.sql_address=b.address
   and a.username in ('FUSION', 'FUSION_RUNTIME')
   and a.sid <> sys_context('USERENV', 'SID');
   ```

3. To retrieve a list of scheduler jobs that are currently running:

   ```
   select owner, job_name
   from dba_scheduler_running_jobs;
   ```

6.3.1.5 Confirm All Oracle Fusion Applications Patch Manager Processes Are Complete

From your operating system, check for processes that are running `fapmgr`, `javaworker`, `adpatch`, `adadmin`, and `adworker`. If a fapmgr session was interrupted, you may need to forcefail and abandon the session as follows:

1. Use the `fapmgr forcefail` command to update the patching tables.

   ```
   (UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh forcefail [-logfile log file name]
   [-loglevel level]
   ```

   ```
   (Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd forcefail [-logfile log file
   name] [-loglevel level]
   ```

   If the `forcefail` command returns "There are no active Oracle Fusion Applications Patch Manager sessions which can be forcibly failed", then skip the next step.

2. Use the `fapmgr abort` command to abandon the session, only if a session is active.

```
(UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh abort [-logfile log file name]
[-loglevel level]

(Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd abort [-logfile log file name]
[-loglevel level]
```

6.3.1.6 Confirm All Oracle Fusion Applications AutoPatch Processes Are Complete

If an Oracle Fusion Applications AutoPatch session is running, you must abandon the session as follows:

Run the following command from *ATGPF_ORACLE_HOME:* (This is the directory under *MW_HOME* that contains the Applications Core code. For more information, see Section 7.1.2, "Running Oracle Fusion Applications AutoPatch".)

```
(Unix) lcm/ad/bin/adpatch.sh abandon=y interactive=n defaultsfile=ATGPF_ORACLE_
HOME/admin/TWO_TASK/defaults.txt logfile=log_file_name

(Windows) lcm\ad\bin\adpatch.exe abandon=y interactive=n defaultsfile=ATGPF_
ORACLE_HOME\admin\LOCAL\defaults.txt logfile=log_file_name
```

The *TWO_TASK* value can be obtained from the `ATGPF_env.properties` file.

The *LOCAL* value can be obtained from the `FUSION_env.properties` file.

6.3.1.7 Confirm All AD Administration Sessions Are Complete

If an AD Administration session is running, you must abandon the session as follows:

1. From *FA_ORACLE_HOME:*

```
(Unix) lcm/ad/bin/adadmin.sh abandon=y interactive=n defaultsfile=FA_ORACLE_
HOME/admin/TWO_TASK/defaults.txt logfile=log_file_name

(Windows) lcm\ad\bin\adadmin.cmd abandon=y interactive=n defaultsfile=FA_
ORACLE_HOME\admin\LOCAL\defaults.txt logfile=log_file_name
```

The *TWO_TASK* and *LOCAL* values can be obtained from the `FUSION_env.properties` file.

2. From *ATGPF_ORACLE_HOME*

```
(Unix) lcm/ad/bin/adadmin.sh abandon=y interactive=n defaultsfile=ATGPF_ORACLE_
HOME/admin/TWO_TASK/defaults.txt logfile=log_file_name

(Windows) lcm\ad\bin\adadmin.cmd abandon=y interactive=n defaultsfile=ATGPF_
ORACLE_HOME\admin\LOCAL\defaults.txt logfile=log_file_name
```

The *TWO_TASK* and *LOCAL* values can be obtained from the `ATGPF_env.properties` file.

6.3.1.8 Steps For Windows Platforms

Follow these steps before you install a Language Pack on Windows platforms.

1. Change the service type from Automatic to Manual for the following services: Node Manager, webtier, GOP, and BI. Restore the service type back to Automatic after Language Pack installation completes.

2. Stop the following services: Node Manager, webtier, GOP, and BI.

3. Reboot the Oracle Fusion Applications host.

4. Release Java Archive File Handles on System Process ID (PID) 4

   On the Windows WebLogic Server, the node manager runs as a service. Since, the `APPLICATIONS_BASE` of Oracle Fusion Applications is in a symbolic folder, some of the jar file handles are loaded by Microsoft Windows System Process ID (PID) 4. The loaded file handles eventually cause Middleware patch application to fail when running the Language Pack Installer. Before starting the Language Pack Installer, make sure the Windows System Process ID (PID) 4 does not have handles to Oracle Fusion Applications jar files.

   Check for file handles using the Windows utility Process Explorer. If file handles exist, make sure the node manager service is not running. If the file handles remain even after shutting down the node manager service, switch the node manager service from Automatic to Manual and reboot the machine to release the file handles.

5. Ensure that the `Server` service is up and running.

6. Increase the `shared_pool_size` in the `init.ora` file. If it seems large enough then improve segmentation in the shared pool by reserving part of the shared pool for large objects using the `SHARED_POOL_RESERVED_SIZE` parameter. The recommended value to start tuning is one third of the shared pool size. You can allow for large objects by using the `SHARED_POOL_RESERVED_MIN_ALLOC` parameter.

6.3.2 Perform Required Backups

The following backups must be performed before you install a Language Pack:

- Back Up Oracle Fusion Applications

- Back Up Applications and System Policies

6.3.2.1 Back Up Oracle Fusion Applications

Back up your entire Oracle Fusion Applications environment by following the steps in "Backing Up and Recovering Oracle Fusion Applications" in the *Oracle Fusion Applications Administrator's Guide*. You should also back up your central inventory.

For additional back up steps that are specific to Windows, refer to Section 5.3.4.5, "Back Up Steps for Windows Platforms".

6.3.2.2 Back Up Applications and System Policies

Back up applications and system policies for each stripe supported by Oracle Fusion Applications. If you do not back up the policies by stripe, you cannot restore the policies from your backup. Oracle Fusion Applications supports the following stripes:

- `fscm_system-jazn-data.xml`: FSCM stripe

- `crm_system-jazn-data.xml`: CRM stripe

- `hcm_system-jazn-data.xml`: HCM stripe

- `bip_jazn-data.xml`: OBI stripe

The following steps explain how to back up the system policies and the four application stripes from an OID OPSS security store to individual XML files. These steps must be performed on the Common Domain.

1. Update the following property in a service instance in the jps-config.xml file to automatically create five XML files, `fscm-policies.xml`, `crm-policies.xml`, `hcm-policies.xml`, `obi-policies.xml` (one for each application stripe), and `global-policies.xml` (for system policies):

```
property name: createNew
value: true/false
default: false
```

Each XML file contains the following skeleton:

```
<?xml version="1.0" ?>
  <jazn-data>
     <jazn-realm default="jazn.com">
     </jazn-realm>
  <policy-store>
     <applications>
     </applications>
  </policy-store>
  <jazn-policy>
  </jazn-policy>
  </jazn-data>
```

2. Copy the existing `jps-config.xml` file (that has configured the policystore.ldap service) to a new file, `myFile-migrate-jps-config.xml`.

3. Open `myFile-migrate-jps-config.xml` for editing and add the following `jpsContexts`:

```
<jpsContext name="<MyOIDSecurityStore">>
  <serviceInstanceRef ref="policystore.ldap"/>
</jpsContext>

<jpsContext name="MyDestinationContextFscm">
  <serviceInstanceRef ref="my.fscm.backup"/>
</jpsContext>

<jpsContext name="MyDestinationContextCrm">
  <serviceInstanceRef ref="my.crm.backup"/>
</jpsContext>

<jpsContext name="MyDestinationContextHcm"
  <serviceInstanceRef ref="my.hcm.backup"/>
</jpsContext>

<jpsContext name="MyDestinationContextObi">
  <serviceInstanceRef ref="my.obi.backup"/>
</jpsContext>

<jpsContext name="MyDestinationContextGlobal">
  <serviceInstanceRef ref="my.global.backup"/>
</jpsContext>
```

4. Add the following service instances to `myFile-migrate-jps-config.xml`:

```
<serviceInstance location="<back-up directory>/fscm-policies.xml"
 name="my.fscm.backup" provider="policystore.xml.provider"/>

<serviceInstance location="<back-up directory >/crm-policies.xml"
 name="my.crm.backup" provider="policystore.xml.provider"/>

<serviceInstance location="<back-up directory> /hcm-policies.xml"
```

```
name="my.hcm.backup" provider="policystore.xml.provider"/>

<serviceInstance location="<back-up directory> /obi-policies.xml"
 name="my.obi.backup" provider="policystore.xml.provider"/>

<serviceInstance location="<back-up directory >/global-policies.xml"
 name="my.global.backup" provider="policystore.xml.provider"/>
```

5. Use the OPSS script `migrateSecurityStore` to backup each application stripe:

```
migrateSecurityStore(type="appPolicies",
configFile="jpsConfigFileLocation", src="srcJpsContext",
dst="dstJpsContext", srcApp="srcAppName")
```

Where:

`jpsConfigFileLocation` is the location of the file `myFile-migrate-jps-config.xml`.

`srcAppName` is the stripe being backed up, such as fscm.

`srcJpsContext` is the name of the context that refers to the OID security store, such as, fscm.

`dstJpsContext` is the name of the context that refers to the XML store, such as, `MyDestinationContextFscm`.

6. Use the OPSS script `migrateSecurityStore` to backup system policies:

```
migrateSecurityStore(type="globalPolicies",
configFile="jpsConfigFileLocation", src="srcJpsContext",
dst="dstJpsContext")
```

Where:

`jpsConfigFileLocation` is the location of the file `myFile-migrate-jps-config.xml`.

`srcJpsContext` is the name of the context that refers to the OID security store, such as, MySourceContext.

`dstJpsContext` is the name of the context that refers to the XML policy store, such as MyDestinationContextGlobal.

For more information, see "Migrating with the Script migrateSecurityStore" in the *Oracle Fusion Middleware Application Security Guide*.

6.3.3 Apply Mandatory Prerequisite Patches

Apply any prerequisite patches listed in the Pre-Installation section of NLS release notes prior to starting Language Pack Installer. Note that the only patches that need to be applied are those that have been added to Oracle Fusion Applications release notes since the last time you applied patches from this list.

6.4 Install a Language Pack

Language packs must be applied during downtime. Oracle recommends that language packs be installed from a machine that is co-located in the same subnetwork as the database server to maximize performance. You must run Language Pack Installer on the primordial host.

This section contains the steps to install a language pack with Language Pack Installer. It contains the following topics:

- Perform the Installation
- Complete the Post Installation Tasks

6.4.1 Perform the Installation

Ensure that the steps in Section 6.2, "Prepare to Install a Language Pack Pre-Down Time" and Section 6.3, "Prepare to Install a Language Pack - During Down Time" are successfully completed. Then follow the steps in this section.

> **Note:** If Language Pack Installer encounter errors, refer to Section 6.5, "Troubleshooting Language Pack Installer Sessions" before clicking any buttons in the Language Pack Installer user interface.

6.4.1.1 Start Language Pack Installer

Start Language Pack Installer from the command line, using specific options to further define the necessary actions. Table 6–4 shows valid options that can be used when running Language Pack Installer.

1. Set the PATH environment variable to include *APPLICATIONS_ BASE*\fusionapps\jdk6 as follows.

```
(Unix) export JAVA_HOME=APPLICATIONS_BASE/fusionapps/jdk6
export PATH=$JAVA_HOME/bin:$PATH

(Windows) set JAVA_HOME=APPLICATIONS_BASE\fusionapps\jdk6
set PATH=%JAVA_HOME%\bin;%PATH%
```

2. Confirm registration of the network location of *FA_ORACLE_HOME*.

   If Oracle Fusion Applications Oracle home directory (*FA_ORACLE_HOME*), which is located under the *APPLICATIONS_BASE*/fusionapps directory, is registered in inventory with a /net path then provide the oraInst.loc location including /net while starting the Language Pack Installer. An example follows:

```
REPOSITORY_LOCATION/installers/fusionapps/Disk1/runInstaller -jreLoc
APPLICATIONS_BASE/fusionapps/jdk6/ -invPtrLoc /net/APPLICATIONS_
BASE/fusionapps/applications/oraInst.loc
```

   If not triggered with /net path, Language Pack Installer copies the -invPtrLoc file to *FA_ORACLE_HOME*. In the example, this results in a copy of the file to itself, which causes a zero byte file. This causes failure during the copy phase when oracle_common patches are applied. For more information, see Section 5.5.2.3, "Inventory Pointer File is Empty".

3. Start Language Pack Installer

```
(UNIX) REPOSITORY_LOCATION/installers/fusionapps/Disk1/runInstaller -addLangs
-jreLoc JAVA_HOME_LOCATION [-invPtrLoc FA_ORACLE_HOME/oraInst.loc]
[-J-DupdateJAZNPolicyStore=true] [-J-Dworkers number_of_workers][-J-DlogLevel
level]

(Windows) REPOSITORY_
LOCATION\installers/fusionapps\Disk1\install\win64\setup.exe -jreLoc JAVA_HOME_
LOCATION -addLangs [-DupdateJAZNPolicyStore=true]
-DcontinueOnError=true [-Dworkers number_of_workers][-J-DlogLevel level]
```

Table 6–4   Language Pack Installer Command Line Options

Option Name	Description	Mandatory
-addLangs	Runs Language Pack Installer to install one language.	Yes.
-jreLoc	Path where the Java Runtime Environment is installed. This option does not support relative paths, so you need to specify the absolute path.	Yes.
-invPtrLoc	The location of an overriding inventory pointer file. If Oracle Fusion Applications Oracle home directory (*FA_ORACLE_HOME*), located under the APPLICATIONS_BASE/fusionapps directory, is registered in inventory with a /net path, then provide the oraInst.loc with /net.	No, use only to override the default location of the inventory pointer file, located in /etc/oraInst.loc. This option can be used only on Unix platforms.
-J-DupdateJAZNPolicyStore= true (-DupdateJAZN PolicyStore for Windows)	Updates the policy store with translated attributes so field descriptions, display names, and other attributes display their translated values.	No, use only when you do not want to use base English.
-J-Dworkers (-Dworkers for Windows)	The number of workers to use for uploading database content. If you provide a value for the number of workers that is outside the calculated range, you are prompted to provide a value that is within the optimal range. If you do not use this option, a calculated optimal value is used.	No, overrides the default number of workers calculated by Language Pack Installer. See "Worker Calculation" in Section 3.1.2, "Patching Database Artifacts".
-debug	Retrieve debug information from Oracle Universal Installer.	No.
-J-DlogLevel (-DlogLevel for Windows)	Records messages in the log file at the level you specify. Enter a value to override the default log level of INFO. See Section 11.1, "Oracle Fusion Applications Patch Manager Logging".	No, default value is INFO.

Example 6–1   Language Pack Installation with no policy store translation

```
(Unix) REPOSITORY_LOCATION/installers/fusionapps/Disk1/runInstaller -addLangs
-jreLoc /server01/appmgr/APPLICATIONS_BASE/fusionapps/jdk6
-invPtrLoc FA_ORACLE_HOME/oraInst.loc

(Windows)  REPOSITORY_LOCATION\installers\fusionapps\Disk1\setup.exe -jreLoc
\server01\appmgr\APPLICATIONS_BASE\fusionapps\jdk6 -addLangs
```

Example 6–2   Language Pack installation with policy store translation

```
(Unix) REPOSITORY_LOCATION/installers/fusionapps/Disk1/runInstaller -addLangs
-jreLoc /server01/appmgr/APPLICATIONS_BASE/fusionapps/jdk6
-invPtrLoc FA_ORACLE_HOME/oraInst.loc -J-DupdateJAZNPolicyStore=true

(Windows)  REPOSITORY_LOCATION\installers\fusionapps\Disk1\setup.exe -jreLoc
\server01\appmgr\APPLICATIONS_BASE\fusionapps\jdk6 -addLangs
-DupdateJAZNPolicyStore=true
```

Example 6–3   Language Pack installation when FA_ORACLE_HOME is registered with a /net path

```
(Unix) REPOSITORY_LOCATION/installers/fusionapps/Disk1/runInstaller -addLangs
-jreLoc /server01/appmgr/APPLICATIONS_BASE/fusionapps/jdk6
-invPtrLoc /net/APPLICATIONS_BASE/fusionapps/applications/oraInst.loc
```

6.4.1.2 Install the Language Pack

Table 6–5 illustrates the tasks that Language Pack Installer runs. For information about log files generated during language pack installation, see Section 6.5.1, "Language Pack Installer Log File Directories".

Table 6–5   Language Pack Installation Screen Sequence

Screen	Description and Action Required
Welcome	Appears when you start Language Pack Installer. This screen does not appear if you restart Language Pack Installer after a failure. The standard Welcome screen is read-only. It contains a navigation pane on the left-hand side that summarizes the tasks the installer will take. Each item in the pane represents an installer screen, which contains prompts for the necessary information.
	Click **Next** to continue.
Installation Location	Specify the location of the existing Oracle Fusion Applications home (*FA_ORACLE_HOME*) where you want to install the language.
	Click **Next** to continue.
Installation Summary	Summarizes the selections you made during this installation session. It includes the Oracle home, required and available disk space, and the language to be installed. Review the information displayed to ensure that the installation details are what you intend.
	To make changes before installing, click **Back** to return to previous screens in the interview.
	Click **Install** to start installing this language.
Installation Progress	Displays a progress indicator that shows the percentage of the installation that is complete and indicates the location of the installation log file. The installation step consists of copying files from the Language Pack to the appropriate Oracle homes. The configuration process starts when the installation progress indicator shows 100 percent.
	Click **Next** to continue.

Table 6–5   (Cont.) Language Pack Installation Screen Sequence

Screen	Description and Action Required
Policy Store Analysis (Note that this screen displays only when the `-J-DupdateJAZNPolicyStore` option is set to `true` with the `runinstaller` command.)	Analysis is enabled for the following stripes: hcm, crm, fscm, and obi. Select the stripes to be analyzed and then click **Run Analysis** to identify any conflicts or deletions. Only the stripes that are included in the language pack are enabled for analysis and the analysis could run for several minutes. After the analysis runs, review the results of the analysis and decide which deployment method you want Language Pack Installer to use for policy store changes to each stripe. Oracle recommends that you select **Apply safe changes only**. This is the safest method unless you have read and totally understood the consequences of the other three options. If you decide to resolve the conflicts or deletions before the actual JAZN upload from Language Pack installer, you should run the Policy Store Analysis step again to get the most accurate analysis report. The choices for deployment method are: ■ Apply safe changes only (choose this method if there are no conflicts) ■ Apply all changes and overwrite customizations ■ Append additive changes ■ Manually resolve conflicts and upload changes using Authorization Policy Manager. If you choose **Apply safe changes only** or **Append additive changes**, then you must review the results of the analysis to manually upload any changes not applied by Language Pack Installer with the choice you selected, after the installation is complete. If you choose **Apply all changes and overwrite customizations**, then you may need to reapply the customizations that are overwritten after the installation is complete. If you choose one of these options, click **Next** after you make your selection. If you choose **Manually resolve conflicts and upload changes using Authorization Policy Manager** (APM), you must pause the installation while you bring up the APM application and upload the changes. For more information, see the "Upgrading Oracle Fusion Applications Policies" chapter in the *Oracle Fusion Middleware Oracle Authorization Policy Manager Administrator's Guide (Oracle Fusion Applications Edition)*. Note the location of the following files: ■ Baseline file: *FA_ORACLE_HOME*/admin/JAZN/*stripe*/baseline ■ Patch file for fscm, crm, and hcm stripes: *FA_ORACLE_HOME/stripe*/deploy/system-jazn-data.xml ■ Patch file for the obi stripe: *FA_ORACLE_HOME*/com/acr/security/jazn/bip_jazn-data.xml When you complete this task in APM, shut down the APM application, return to Language Pack Installer, and click **Next**.

Table 6–5   (Cont.) Language Pack Installation Screen Sequence

Screen	Description and Action Required
Configuration Progress	Displays a progress indicator that shows the percentage of the configuration that is complete. It displays each task in the message pane as it is performed. Tasks that could be included in the configuration phase are described in Section 6.1.5, "Language Pack Installer Configuration Tasks".
	Before the **Starting All Servers** task, the **Verifying Node Manager and OPMN Status** configuration task checks for access to the Node Manager and the OPMN control process. Do not cancel and exit out of Language Pack Installer in response to this task.
	If starting of servers time out, see Section 5.5.16, "Failures During Starting All Servers".
	No additional user action is required in the Configuration Progress screen unless a failure occurs.
Installation Complete	Summarizes the installation just completed. If you want to save this configuration to a response file, click **Save**. For more information, see "How Response Files Work" in the *Oracle Database Installation Guide 11g Release 2 (11.2) for Linux*.
	To complete a successful installation, click **Finish**. The **Finish** button is activated only if all mandatory configuration tasks completed successfully. If you want to rerun this session after you resolve failed configuration tasks, click **Cancel.**

6.4.2 Complete the Post Installation Tasks

Perform the following required manual steps after Language Pack Installer completes successfully:

1. Confirm that all deployments were successful by reviewing the Diagnostics report and log files. For more information, see Section 3.5.5, "Diagnostics Report".

2. Confirm there are no unresolved errors or exceptions in the log files. For information about resolving errors, see Section 6.5, "Troubleshooting Language Pack Installer Sessions".

3. Confirm that all relevant Managed Servers have a RUNNING status.

4. Verify that all deployed applications are up and running. You can check this from Fusion Applications Control, or by reviewing the server side log files. For more information, see "Starting Fusion Applications Control" in the *Oracle Fusion Applications Administrator's Guide* or Section 6.5.1, "Language Pack Installer Log File Directories".

5. Review the JAZN Analyze report for potential conflicts and deletions that are not patched automatically by Language Pack Installer.

   FA_ORACLE_HOME/admin/JAZN/*stripe*/delta/report.txt

   The *stripe* is crm, fscm, hcm, or obi.

   Review the Modification section of the report to see the roles that Language Pack Installer did not update. For each conflict that displays in this report, you must evaluate and manually patch the role by using APM. For more information, see "Upgrading Oracle Fusion Applications Policies" in the *Oracle Fusion Middleware Oracle Authorization Policy Manager Administrator's Guide (Oracle Fusion Applications Edition)*.

The following example shows a typical Applications Role conflict that has been modified by both the patch and production, therefore it will not be applied by Language Pack Installer.

```
MODIFICATION CONFLICTS
Artifact type: Application Role
Artifact Name: OBIA_PARTNER_CHANNEL_ADMINISTRATIVE_ANALYSIS_DUTY
Description: This artifact is modified at attribute level in patch version and
also in production.
```

Note the location of the following files for reference when using APM:

- Location of baseline files, where stripe is crm, fscm, hcm, or obi:

   `FA_ORACLE_HOME/admin/JAZN/stripe/baseline`

- Location of patch files for fscm, crm, and hcm stripes:

   `FA_ORACLE_HOME/stripe/deploy/system-jazn-data.xml`

- Location of patch files for the obi stripe:

   `FA_ORACLE_HOME/com/acr/security/jazn/bip_jazn-data.xml`

6. Perform any steps listed in the Post-Installation Tasks section of NLS Release Notes.

6.5 Troubleshooting Language Pack Installer Sessions

This section provides information to assist you in troubleshooting Language Pack Installer sessions specifically. For troubleshooting issues that are generic to both RUP Installer and Language Pack Installer, see Section 5.5, "Troubleshoot RUP Installer Sessions".

This section contains the following topics:

- Language Pack Installer Log File Directories
- Failure During the Installation Phase
- Warning Message About "no translations/fsm patches for atgpf"

6.5.1 Language Pack Installer Log File Directories

Table 6–6 contains a list of log directories for Language Pack Installer activities.

Table 6–6   Log Directories for Language Pack Installer Activities

Log directory name	Generated from...
oracle_inventory/oraInstall_*timestamp*/log	Installation phase
FA_ORACLE_HOME/admin/FUSION/log/fapatch/fapatch_ language_11.1.3.0.0	Top level directory for Language Pack Installer logs
FA_ORACLE_HOME/admin/FUSION/log/fapatch/fapatch_ *language*_11.1.3.0.0/PatchManager_DBPatch	Configuration phase when database actions run
FA_ORACLE_HOME/admin/FUSION/log/fapatch/fapatch_ *language*_11.1.3.0.0/ActivateLanguage	Configuration phase when language is activated
FA_ORACLE_HOME/admin/FUSION/log/fapatch/fapatch_ *language*_11.1.3.0.0/Startstop	StartStop utility

Table 6–6   (Cont.) Log Directories for Language Pack Installer Activities

Log directory name	Generated from...
FA_ORACLE_HOME/admin/FUSION/log/fapatch/fapatch_ *language*_11.1.3.0.0/soalogs	SOA Composite activities
	Note that SOA server logs are located under respective domains. For example, the SOA server logs for CommonDomain are under *APPLICATIONS_ CONFIG*/domains/*hostname*/Com monDomain/servers/soa_ server1/logs. For more information, see Section 5.5.19.1, "SOA Composite Log Files".

6.5.2 Failure During the Installation Phase

Follow these steps when an error occurs during the installation phase:

1. Click **Cancel** to exit Language Pack Installer.

2. Review the log files to determine the cause of the failure. The installation log files reside in the *FA_ORACLE_HOME*/admin/FUSION/log/fapatch/fapatch_ language_11.1.3.0.0 directory.

3. Resolve the cause of the failure.

4. Start Language Pack Installer using the same command syntax that you used for the previous incomplete installation. For more information, see Section 6.4.1, "Perform the Installation". After canceling the previous installation and starting again, you must choose to continue with the previous failed installation by clicking **Yes** on the Checkpoint Dialog. If the error is not recoverable, you can restore and restart from backup.

5. If you choose to continue with the failed installation, Language Pack Installer opens at the screen where it was canceled. When canceled during the copy action, it relaunches in the Installation Summary screen. Click **Next** to navigate through the Installation Summary screen. When the Installation Progress screen displays, click **Install** to start the installation again.

6.5.3 Warning Message About "no translations/fsm patches for atgpf"

When applying a language pack, you may notice the following error in the Apply Middleware patches log:

```
There are no translations/fsm patches for atgpf at
REPOSITORY_LOACTION\atgpf\dbpatch\translations\fsm\F
```

You can ignore this message.

6.6 Maintaining Languages

Oracle Fusion Applications content is translated to different languages and fixes are made available as individual patches. If your environment uses multiple languages, whenever you apply a patch with translatable content, you may choose to also apply the associated translated patch for each of your installed languages. If a patch does not contain any translated content, such as a PL/SQL package, only the English patch is available.

If an Oracle Fusion Applications environment contains languages other than English, the recommended method for applying patches is to apply the English patch first and

then apply the translation patch for each installed language.For example, after you apply a language pack for another language, such as Korean, whenever you apply a patch that involves translatable content, you must apply the base English patch and also the Korean patch for that fix.

For detailed information about how to apply a patch, see Section 3.4, "Applying Patches".

7

Patching Oracle Fusion Middleware Extensions for Applications

This chapter describes how to apply patches to update Oracle Fusion Middleware Extensions for Applications (Applications Core).

This chapter contains the following topics:

- Patching Applications Core Database Artifacts
- Patching Applications Core Middleware Artifacts
- Log Files
- Monitoring and Troubleshooting Applications Core Patching Sessions
- Performing System Maintenance Tasks

7.1 Patching Applications Core Database Artifacts

The same set of patching related software and database tables is used by both Oracle Fusion Applications Patch Manager and Oracle Fusion Middleware Extensions for Applications (Applications Core). Oracle Fusion Applications Patch Manager and Applications Core each have their own separate Oracle home. Product specific shell scripts used for database patching exist in each corresponding Oracle home location. The separate scripts are provided in order to support each product's individual patching requirements. The scripts are uniquely defined to reference the appropriate Oracle home, set the patching configuration and environment, and then call the appropriate utility for patching.

Oracle Fusion Applications Patch Manager automatically calls Oracle Fusion Applications AutoPatch when it detects patch metadata that indicates a patch contains database content. However, you run Oracle Fusion Applications AutoPatch directly to apply an applications database patch for Applications Core.

Oracle Fusion Applications AutoPatch is used to apply patches that contain fixes or updates to applications database artifacts. It gathers the necessary information about the applications system and performs the following tasks required to apply a patch:

- Reads patch metadata to determine patch dependencies and requirements
- Uploads patch information from a prior patch session to the database (if needed)
- Reads and validates the patch driver file
- Compares version numbers of object modules from the product libraries and version numbers of the existing files against the patch files
- Backs up all existing files that will be changed by the patch

- Copies files

- Updates database objects

- Saves patch information to the database

- Takes no action if a patch contains no new updates to files or database objects in your system

- Detects if there is a previously failed Oracle Fusion Applications AutoPatch session and attempts to recover that session

7.1.1 Artifacts Supported by Oracle Fusion Applications AutoPatch

Table 7–1 lists the types of artifacts that are supported by Oracle Fusion Applications AutoPatch.

Table 7–1   Database Artifacts Supported by Oracle Fusion Applications AutoPatch

Artifact Type	Description	Patching Recommendations
Applications Seed Data (XML,XLF files)	Examples include static lists of values, functional or error messages, and lookup values. Any non-transactional data values loaded into your database can be considered seed data.	Oracle recommends that patches containing seed data be applied from a machine that is co-located in the same subnetwork as the database server to maximize performance.
Applications Database schema changes (SXML files)	Examples include tables, triggers, views, sequences, synonyms, queues, queue tables, policies, and contexts.	None
PL/SQL objects (PDQ, PCB files)	Package headers and bodies.	Manually shut down the Oracle Enterprise Scheduler Service servers before applying patches that contain PL/SQL changes.
SQL scripts	Scripts that update the database.	None

7.1.2 Running Oracle Fusion Applications AutoPatch

You run Oracle Fusion Applications AutoPatch by using the command line utility, adpatch, located in the *ATGPF_ORACLE_HOME*/lcm/ad/bin directory. This is the directory under MW_HOME that contains the Applications Core code. The utility's shell script sets the environment for *ATGPF_ORACLE_HOME* and calls the utility. For UNIX, the shell script is adpatch.sh and for Windows, it is adpatch.exe. You direct the way adpatch operates by adding arguments and options to the command. Command line arguments use the token=value format.

The following command shows the basic syntax for the adpatch utility:

```
(UNIX) ATGPF_ORACLE_HOME/lcm/ad/bin/adpatch.sh patchtop=complete_path_to_unzipped_
patch_directory \
driver=driver_name workers=number_of_workers [optional arguments=value]

(Windows) ATGPF_ORACLE_HOME\lcm\bin\adpatch.exe patchtop=complete_path_to_
unzipped_patch_directory \
driver=driver_name workers=number_of_workers [optional arguments=value]
```

Table 7–2 displays the arguments used by Oracle Fusion Applications AutoPatch:

Table 7–2   Arguments Used by Oracle Fusion Applications AutoPatch

Argument	Description	Mandatory	Default Value	Example
abandon	Abandons a failed patching session	No	n for no	abandon=y
apply	Applies the patch	No	y for yes	apply=n
backup	Allows you to override the backup directory for files that are copied	No	*ATGPF_ ORACLE_ HOME*/admin/ pbackup	backup=*ATGPF_ ORACLE_HOME*/admin
defaults file	File delivered by Oracle that contains the environment information required to apply a patch	Recommended	None	defaultsfile=ATGPF_ ORACLE_ HOME/admin/TWO_ TASK/defaults.txt
driver	Name of the patch driver file	Yes	None	driver=u*patch_ number*.drv
help	Accesses help for adpatch	No	n for no	help=y
interactive	Allows you to apply a patch non-interactively using information from the defaults file	Yes	y for yes	interactive=n
logfile	Name for log file	No	adpatch_ apply.log	logfile=adpatch_apply_ *patch_number*.log
loglevel	Records messages in the log file at the level you specify. Enter a value to override the default log level of INFO. See Section 11.1, "Oracle Fusion Applications Patch Manager Logging"	No	NOTIFICATIO N:16	loglevel=WARNING
logtop	Top level directory where log files are written	No	*ATGPF_ ORACLE_ HOME*/admin/F USION/log	logtop=/tmp/admin/lo g
max_trial_ time	The maximum time in minutes that deferred tasks are attempted	No	10 minutes	max_trial_time=5
parallel_ index_ threshold	Threshold block count in each table, which when exceeded for a tables, causes its indexes to be created using parallel slaves	No	10000	parallel_index_ threshold=12000
patchtop	Top level directory for the unzipped patch	Yes	None	patchtop=/temp/patche s/*patch_number*
printdebug	Displays additional debug information	No	n for no	printdebug=y
restart	Resumes a failed patching session	No	None	restart=y

Table 7–2   (Cont.) Arguments Used by Oracle Fusion Applications AutoPatch

Argument	Description	Mandatory	Default Value	Example
wait_on_failed_job	Waits for user intervention when all tasks fail. If set to no, AutoPatch exits when all tasks assigned to workers have failed and require user intervention.	Recommended	n for no	wait_on_failed_job=y
workers	Number of workers to use for database patching tasks	Yes	None	workers=8

To access help for the adpatch command, type adpatch help=y. The output of the help argument provides a list of the options you can use to refine the operation of adpatch, along with a brief description of each option.

7.1.2.1 Applying Patches Non-interactively

Oracle Fusion Applications AutoPatch should be run non-interactively from the command line by using the defaults.txt file that contains the information required to apply the patch. During the installation and configuration for Applications Core, the defaults.txt file is created in this location: *ATGPF_ORACLE_HOME*/admin/TWO_TASK/defaults.txt. Note that TWO_TASK is the name of the database to which you are applying the patch.

7.1.2.2 End-to-End Patching Process

The end-to-end process of applying individual patches using Oracle Fusion Applications AutoPatch, includes the following steps.

> **Note:**   As part of the patching process, customers have their own backup and recovery management process. Oracle recommends that you always have a current backup before applying a patch.

> **Note:**   There can be only one patching session active for Oracle Fusion Applications and Applications Core at a time.

Step 1 Research Issue that Needs to be Resolved by a Patch

When you have an issue that needs to be resolved by a patch for Applications Core, file a service request with Oracle Support Services or research the issue on My Oracle Support:

http://support.oracle.com

Step 2 Obtain and Unzip the Patches

Upon determining that you need new patches, download the patches from My Oracle Support. Unzip the patch ZIP files in your PATCH_TOP directory. PATCH_TOP can be any location in your file system.

Step 3 Read the README File

Read the README file that accompanies each patch. This file contains important information and instructions that must be followed.

If a patch contains preinstallation or postinstallation manual steps, they are described in the patch README file.

Step 4 Prepare the System

To prevent locks on patched objects and other data issues during patching of database artifacts, review and perform the following checklist before patching the target database system:

- Confirm that the database system is in an idle state

- Confirm that there are no active jobs or processes running against the database

- Stop all background jobs, including jobs in the database and active processes

- Manually shut down the Oracle Enterprise Scheduler Service (ESS) servers, especially when a patch contains a PL/SQL package, by performing the following steps:

    a. Stop the ESS request processor and dispatcher to prevent new requests from being processed. See "Starting and Stopping a Request Processor or Dispatcher" in the *Oracle Fusion Applications Administrator's Guide* for more information.

    b. Cancel any in-progress requests. See "Cancelling Oracle Enterprise Scheduling Service Job Requests" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Enterprise Scheduling Service* for more information.

    c. Shutdown the ESS WebLogic Server Managed server. See the "Starting and Stopping" table, specifically the "Managed Server for an application" row, in the *Oracle Fusion Applications Administrator's Guide* for more information.

Step 5 Apply the Prerequisite Patches

If any prerequisite patches are required, as described in the README file, apply those patches with Oracle Fusion Applications AutoPatch.

Step 6 Identify the correct Oracle home

Identify the Applications Core Oracle home (*ATGPF_ORACLE_HOME*). This is the directory under *MW_HOME* that contains the Applications Core code.

Step 7 Apply the Patch

Apply the patch using the `adpatch` command. An example of the `adpatch` command follows:

```
(UNIX) FA_ORACLE_HOME/lcm/ad/bin/adpatch.sh defaultsfile=ATGPF_ORACLE_
HOME/admin/TWO_TASK/defaults.txt \
patchtop=complete_path_to_unzipped_patch driver=upatch_number.drv \
workers=number_of_database_workers interactive=no [logfile=log_file_name]\
[logtop=ATGPF_ORACLE_HOME/admin/FUSION] [loglevel=level] wait_on_failed_job=yes

(Windows) FA_ORACLE_HOME\lcm\ad\bin\adpatch.exe defaultsfile=ATGPF_ORACLE_
HOME\admin\TWO_TASK\defaults.txt \
patchtop=complete_path_to_unzipped_patch driver=upatch_number.drv \
workers=number_of_database_workers interactive=no [-ogfile=log_file_name]\
[logtop=ATGPF_ORACLE_HOME\admin\FUSION] [loglevel=level] wait_on_failed_job=yes
```

Step 8 Monitor the Application of the Patch

You can monitor the progress of the patching session and verify its successful completion by using the AD Controller utility. For more information, see Section 7.4, "Monitoring and Troubleshooting Applications Core Patching Sessions".

Step 9 Review the Log Files

Review the log files when the patch session is complete. For more information, see Section 7.3, "Log Files".

Step 10 Apply Postinstallation Patches or Run Manual Steps

If any postinstallation patches are required, as indicated in the README file, apply them. Run any manual steps that are described in the README file.

7.2 Patching Applications Core Middleware Artifacts

You use the OPatch utility to patch Applications Core middleware artifacts. All patches are available for download from My Oracle Support.

To patch Applications Core middleware artifacts

1. Identify the Applications Core Oracle home (*ATGPF_ORACLE_HOME*). This is the directory under *MW_HOME* that contains the Applications Core code.

2. Set the *ORACLE_HOME* to *ATGPF_ORACLE_HOME*.

    Example:

    ```
    setenv ORACLE_HOME /server01/mwhome/Oracle_atgpf
    ```

    Or:

    ```
    export ORACLE_HOME=/server01/mwhome/Oracle_atgpf
    ```

3. Create a temporary directory to stage the Applications Core patches.

    ```
    mkdir Temp_Directory
    ```

4. Unzip the OPatch patches in the temporary directory.

5. Review the README.txt file for information about any preinstallation and postinstallation steps.

6. Apply the patches using OPatch:

    ```
    cd patch_top_directory
    ORACLE_HOME/OPatch/opatch apply -invPtrLoc ORACLE_HOME/oraInst.loc
    ```

    For more information about OPatch, see "Patching Oracle Fusion Middleware with Oracle OPatch" in the *Oracle Fusion Middleware Patching Guide*.

7. Stop and start the WebLogic server. For more information, see "Starting and Stopping a Product Family Oracle WebLogic Server Domain" in the *Oracle Fusion Applications Administrator's Guide*.

8. Stop and start the Administration Server and all Managed Servers. For more information, see "Starting and Stopping" in Oracle Fusion Applications Administrator's Guide.

9. Run the postinstallation steps, if applicable.

10. Apply the 'Deployment of Fusion APPS Attachments in UCM server OPatch' patch to your *ECM_ORACLE_HOME*. Follow the same instructions in Steps 1 through 9 to apply this patch.

7.2.1 Patching Global Menus in FndSetup

MAR artifacts that contain Global Menus are delivered in Applications Core OPatch patches and copied to this location when you apply the patch using OPatch:.

```
ATGPF_ORACLE_HOME/atgpf/applications/exploded/FndSetup.ear/FndAppsMenuData.mar
```

After you apply the patch with OPatch, you must copy this MAR artifact to a specific location in *FA_ORACLE_HOME* and start the corresponding Managed Server. Use the following example syntax to copy the file:

```
cp ATGPF_ORACLE_HOME/atgpf/applications/exploded/FndSetup.ear/FndAppsMenuData.mar
FA_ORACLE_HOME/fusionapps/applications/fs/deploy/FndSetup.ear
```

7.2.2 Patching the Flexfield SOA Synch Composite

Extensible flexfields require synchronization between the Service Oriented Architecture (SOA) Metadata Service (MDS) and Oracle Fusion Applications MDS, which is delivered in the `sca_UpdateSOAMDS_rev_number.jar` file. When updates to this jar are delivered in a patch, you must manually deploy the SOA composite after you apply the patch using OPatch. To deploy the SOA composite, log in to Oracle Fusion Applications Control as the WebLogic user, navigate to **SOAServer** and select **Deploy**.

7.3 Log Files

Oracle Fusion Applications AutoPatch creates log files in the *ATGPF_ORACLE_HOME*/admin/FUSION directory. You specify the name of the main log file by using the `logfile` argument when you run Oracle Fusion Applications AutoPatch. The related log files are named based on the name of the main log file. For example, if the name of the main log file is `adpatch_123456_apply.log`, then the worker logs for the session are named `adpatch_123456_apply_worker_worker_number`.log.

Table 7–3 displays the Oracle Fusion Applications AutoPatch log files.

Table 7–3   Log Files for Oracle Fusion Applications AutoPatch

Log file name	Log file description
adpatch.log	Main log file; Oracle recommends you override the default name by including the patch number in the name of the log file.
adpatch.lgi	Contains informational messages.
adlibin.log	Contains information about moving C object files into the C library.
adlibout.log	Contains information about moving C object files out of the C library.
adpatch_worker*workernumber*.log	Worker log files for database tasks that run in parallel.
*language_filename*_ldt.log	Seed data loader files.

7.4 Monitoring and Troubleshooting Applications Core Patching Sessions

The AD Controller utility, `adctrl`, can monitor, determine the status, and control the progress of the workers called by Oracle Fusion Applications AutoPatch to update database content. For more information about workers, see Section 3.1.2.1, "Worker Processes".

The AD Controller utility can monitor database patching sessions that were started by both Oracle Fusion Applications AutoPatch and Oracle Fusion Applications Patch Manager. To start `adctrl` to monitor Applications Core patching sessions, make sure you start the session in *ATGPF_ORACLE_HOME*.

The following sections offer steps for troubleshooting issues that may occur during patching sessions for database content.

- Starting AD Controller
- Reviewing Worker Status
- Determining Why a Worker Failed
- Restarting a Failed Worker
- Restarting a Failed Patching Session
- Abandoning a Failed Patching Session
- Applying a Patch to the Wrong Oracle Home

7.4.1 Starting AD Controller

Follow these steps to start AD Controller:

1. Start AD Controller with the `adctrl` command.

   ```
   (UNIX) FA_ORACLE_HOME/fusionapps/atgpf/lcm/ad/bin/adctrl.sh
   (Windows) FA_ORACLE_HOME\fusionapps\atgpf\lcm\ad\bin\adctrl.cmd
   ```

   It prompts you to:

   - Confirm the value of the Applications Core Oracle home
   - Specify an AD Controller log file. This log file is written to the current working directory. The default is `adctrl.log`.

2. After the main menu displays, enter a number to select an option. You can press **Enter** at any time to return to the AD Controller main menu.

7.4.2 Reviewing Worker Status

When Oracle Fusion Applications AutoPatch or AD Administration runs tasks in parallel, it assigns tasks to workers for completion. There may be situations that cause a worker to stop processing. You can use AD Controller to determine the status of workers and manage worker actions.

Follow these steps to review the status of the workers from AD Controller:

1. Start AD Controller. For more information, see Section 7.4.1, "Starting AD Controller".

2. Review worker status.

Select **Show worker status** from the AD Controller main menu. AD Controller displays a summary of current worker activity. The summary columns are:

- Control Worker: The worker number

- Code: The last instruction from the manager to the worker

- Context: The general action the manager is executing

- Filename: The file the worker is running, if any

- Status: The status of the worker

  Table 7–4 describes the status that may be assigned to a worker.

Table 7–4   Worker Status

Status	Meaning
Assigned	The manager assigned a task to the worker and the worker has not yet started.
Completed	The worker completed the task and the manager has not yet assigned it a new task.
Failed	The worker encountered a problem.
Fixed, Restart	You fixed the problem, and the worker will retry the task that failed.
Restarted	The worker is retrying a task or has successfully restarted a task. Note that the status does not change to Running.
Running	The worker is running a task.
Wait	The worker is idle.

If the worker shows a status of Failed, refer to Section 7.4.3, "Determining Why a Worker Failed" for assistance in fixing the problem so Oracle Fusion Applications AutoPatch can complete its processing.

7.4.3 Determining Why a Worker Failed

When a worker fails its task, you do not have to wait until the other workers and the manager stop. You can review the worker log files to determine what caused the failure. Workers do not proceed to run tasks in the subsequent phase until all tasks in the current phase complete successfully. You must take action to resolve the failure so the workers can continue to run tasks in the next phase. If the task was deferred after the worker failed, there may be no action required from you.

The first time a task fails, the manager defers the task and assigns the worker a new task. If the deferred task fails a second time, the manager defers it a second time only if the runtime of the task is less than 10 minutes. If the deferred task failed a third time, or if its runtime is greater than 10 minutes, the task stays at a failed status and the worker waits for manual intervention. Action by you is then required because the worker stops any further processing.

Follow these steps to find out why a worker failed:

1. Follow the steps in Section 7.4.2, "Reviewing Worker Status" to find the worker number that failed.

2. Open and review the log file for the failed worker to determine the cause of the worker failure.

Each worker logs the progress of tasks assigned to it in `adpatch_`
`worker`*workernumber*`.log`. The worker log file contains information that
describes exactly what task it was running and what error occurred that resulted
in a failure. Review the worker log file for the failed worker to determine the
source of the error. For more information, see Section 7.3, "Log Files".

3. Determine how to fix the problem that caused the failure.

Resolve the error using the information provided in the log files. Search for the
resolution at the My Oracle Support site or file a service request with Oracle
Support Services if you do not understand how to resolve the issue.

4. After you resolve the problem that caused the failure, restart the failed worker.

Select **Tell worker to restart a failed job** from the AD Controller main menu to tell
the worker to restart the failed task. For more information, see Section 7.4.4,
"Restarting a Failed Worker".

5. Verify the worker status.

Select **Show worker status** from the AD Controller main menu. The Status column
for the worker that failed should now display Restarted or Fixed, Restart.

7.4.4 Restarting a Failed Worker

If a worker job failed or if you terminated a hanging worker process, you must
manually restart the worker. Some worker processes spawn other processes called
child processes. If you terminate a child process that is hung, the worker that spawned
the process shows *Failed* as the status. After you fix the problem, you must restart the
failed worker. After the worker restarts, the associated child processes start as well.

Follow these steps to restart a failed worker:

1. Start AD Controller. For more information, see Section 7.4.1, "Starting AD
Controller".

2. Select **Show worker status** from the AD Controller main menu.

3. Take the appropriate action for each worker status:

- If the worker status is Failed and its job has failed, select **Tell worker to restart
a failed job**. When prompted, enter the number of the worker that failed.

- If the worker status is Running or Restarted, but the job is hung, follow the
steps in Section 11.5.5, "Terminating a Hung Worker Process".

The worker will restart its assigned tasks and spawn the associated child
processes.

7.4.5 Restarting a Failed Patching Session

If your patch session failed, you can restart the session after you resolve the issue that
caused the failure. Use the `restart` argument, as shown in the following example:

```
(UNIX) FA_ORACLE_HOME/lcm/ad/bin/adpatch.sh defaultsfile=ATGPF_ORACLE_
HOME/admin/TWO_TASK/defaults.txt \
patchtop=/mypatches/1213456 driver=u123456.drv workers=8 \
interactive=n logfile=adpatch_apply_123456.log loglevel=WARNING]\
logtop=ATGPF_ORACLE_HOME/admin/FUSION wait_on_failed_job=y restart=y

(Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd defaultsfile=ATGPF_ORACLE_
HOME\admin/TWO_TASK\defaults.txt \
patchtop=\mypatches\123456 driver=u123456.drv workers=8 \
```

```
interactive=no logfile=adpatch_apply_123456.log loglevel=WARNING \
logtop=ATGPF_ORACLE_HOME\admin\FUSION wait_on_failed_job=yrestart=y
```

7.4.6 Abandoning a Failed Patching Session

If your patch session failed and you do not want to restart it, you must abandon the session to update the database tables, allowing you to start a new patch session. Use the `abandon` argument, as shown in the following example:

```
(UNIX) FA_ORACLE_HOME/lcm/ad/bin/adpatch.sh defaultsfile=ATGPF_ORACLE_
HOME/admin/TWO_TASK/defaults.txt \
patchtop=/mypatches/1213456 driver=u123456.drv \
interactive=no logfile=adpatch_abandon_123456.log loglevel=WARNING\
logtop=ATGPF_ORACLE_HOME/admin/FUSION abandon=y

(Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd defaultsfile=ATGPF_ORACLE_
HOME\admin/TWO_TASK\defaults.txt \
patchtop=/mypatches/1213456 driver=u123456.drv \
interactive=no logfile=adpatch_abandon_123456.log loglevel=WARNING\
logtop=ATGPF_ORACLE_HOME\admin\FUSION abandon=y
```

> **Note:** There can be only one patching session active for Oracle Fusion Applications and Oracle Middleware Extensions for Applications at a time. If there is a failed Oracle Fusion Applications Patch Manager session, see Section 11.3.2, "Abandoning a Failed Patching Session".

7.4.7 Applying a Patch to the Wrong Oracle Home

You must apply Applications Core patches to the correct Oracle home. For example, if you try to apply an Applications Core patch to the Oracle Fusion Applications Oracle home, you receive this error message:

```
Error: Incompatible Patch.
 Cannot apply ATGPF patch on FA_ORACLE_HOME
```

To resolve this issue, ensure that you are applying the patch to *ATGPF_ORACLE_HOME*.

7.5 Performing System Maintenance Tasks

AD Administration is a standalone utility that performs administration maintenance tasks for the products in your Applications Core Oracle home. The general purpose of the maintenance tasks is to keep your Applications Core files and database objects up-to-date. Some maintenance tasks should be performed systemwide on a regular basis, while others are required infrequently.

Run AD Administration by using the command-line utility, `adadmin`. This utility has a shell script that sets the environment and calls the utility. For UNIX, the shell script is `adadmin.sh` and for Windows it is `adadmin.cmd`. To run AD Administration for Applications Core, use this command syntax:

```
(UNIX) FA_ORACLE_HOME/fusionapps/atgpf/lcm/ad/bin/adadmin.sh [argument]
(Windows) FA_ORACLE_HOME\fusionapps\atgpf\lcm\ad\bin\adadmin.cmd [argument]
```

Refer to Chapter 10, "Performing System Maintenance Tasks" for how to use AD Administration. This chapter describes using AD Administration for both

Applications Core and Oracle Fusion Applications Patch Manager. The only difference is the location of the command you use to start AD Administration.

8

Patching Oracle Fusion Functional Setup Manager

This chapter describes how to apply patches to update Oracle Fusion Functional Setup Manager.

This chapter contains the following topics:

- Introduction to Oracle Fusion Functional Setup Manager
- Patching Functional Setup Manager Database Artifacts
- Patching Functional Setup Manager Middleware Artifacts
- Log Files
- Monitoring and Troubleshooting Patching Sessions
- Performing System Maintenance Tasks

8.1 Introduction to Oracle Fusion Functional Setup Manager

Oracle Fusion Functional Setup Manager enables rapid and efficient planning, implementation, and deployment of Oracle Fusion Applications through self-service administration. The code for Functional Setup Manager is maintained in the `ATGPF_ORACLE_HOME` for Oracle Fusion Applications

8.2 Patching Functional Setup Manager Database Artifacts

The same set of patching related software and database tables is used by both Functional Setup Manager and Oracle Fusion Middleware Extensions for Applications (Applications Core). You run Oracle Fusion Applications AutoPatch directly to apply an applications database patch for Functional Setup Manager. For more information, see Section 7.1, "Patching Applications Core Database Artifacts". The patch README file for Functional Setup Manager patches contains information to assist you in performing the patching steps correctly.

8.2.1 Database Artifacts Supported for Functional Setup Manager

Table 8–1 lists the types of artifacts that are supported for Functional Setup Manager.

Table 8–1   Database Artifacts Supported for Functional Setup Manager

Artifact Type	Description	Patching Recommendations
Applications Seed Data (XML,XLF files)	Examples include static lists of values, functional or error messages, and lookup values. Any non-transactional data values loaded into your database can be considered seed data.	Oracle recommends that patches containing seed data be applied from a machine that is co-located in the same subnetwork as the database server to maximize performance.
Applications Database schema changes (SXML files)	Examples include tables, triggers, views, sequences, synonyms, queues, queue tables, policies, and contexts.	

8.2.2 Patching the Functional Setup Manager Database

To apply a Functional Setup Manager database patch, follow the steps in Section 7.1.2, "Running Oracle Fusion Applications AutoPatch".

8.3 Patching Functional Setup Manager Middleware Artifacts

Functional Setup Manager requires middleware artifacts that are deployed on the WebLogic Server. You use OPatch to apply a patch to update Functional Setup Manager artifacts.

8.3.1 Middleware Artifacts Required by Functional Setup Manager

Functional Setup Manager requires certain middleware artifacts that may need to be patched. Table 8–2 displays these middleware artifacts along with actions that need to be performed manually after you apply the patch and what must be running while you apply the patch and perform the manual actions.

Table 8–2   Oracle Fusion Middleware Artifacts Required by Functional Setup Manager

Artifact Type	Actions to Be Performed Manually	What Must Be Running During Patching and Manual Actions
Oracle ADF JAR	Start and stop the relevant servers that host the Java EE application.	Administration Server, node manager, database, LDAP.
Oracle Business Intelligence Publisher (Reports and Captions)	Shut down the BI Presentation server before patching, deploy to Business Intelligence repository, and start the BI Presentation server after patching.	Shut down the BI presentation server before patching. See Section 4.4, "Patching Oracle Business Intelligence Publisher Artifacts".
Oracle Enterprise Scheduler Service MAR	Stop and start the relevant servers that host the Java EE application.	Administration Server, node manager, database.

8.3.2 Patching Functional Setup Manager Middleware Artifacts

You use the OPatch utility to patch Functional Setup Manager middleware artifacts. The patch README file for Functional Setup Manager patches contains information to assist you in performing the patching steps correctly.

For more information, see Section 7.2, "Patching Applications Core Middleware Artifacts".

8.3.3 How to Patch Applications Policies (jazn-data.xml)

The following steps must be performed if you patch applications policies.

1. Back up function security policies in the Oracle Internet Directory (OID) Policy store by following the steps in "Prerequisites to Patching Policies" in the *Oracle Fusion Middleware Oracle Authorization Policy Manager Administrator's Guide (Oracle Fusion Applications Edition)*.

2. Deploy on the FSCM policy stripe using Oracle Authorization Policy Manager. The jazn files are available in ATGPF_ORACLE_HOME/setup and ATGPF_ ORACLE_HOME/setupEss directories. For more information, see "Upgrading Oracle Fusion Applications Policies" in *Oracle Fusion Middleware Oracle Authorization Policy Manager Administrator's Guide (Oracle Fusion Applications Edition)*. Note that FSM is only one of the components in the FSCM stripe and there are other components in the same stripe that you should not update.

8.4 Log Files

Oracle Fusion Applications AutoPatch creates log files in the `ATGPF_ORACLE_ HOME`/admin/APPLCORE directory. For more information, see Section 7.3, "Log Files".

8.5 Monitoring and Troubleshooting Patching Sessions

The AD Controller utility, `adctrl`, can monitor and control the progress of the workers called by Oracle Fusion Applications AutoPatch to update database content. For more information, see Section 7.4, "Monitoring and Troubleshooting Applications Core Patching Sessions".

8.6 Performing System Maintenance Tasks

AD Administration is a standalone utility that performs administration maintenance tasks for the products in `ATGPF_ORACLE_HOME`. The general purpose of the maintenance tasks is to keep your `ATGPF_ORACLE_HOME` files and database objects up-to-date. Some maintenance tasks should be performed systemwide on a regular basis, while others are required infrequently. For more information, see Section 7.5, "Performing System Maintenance Tasks".

9

Patching Oracle Fusion Applications Functional Core

This chapter describes how to apply patches to update Oracle Fusion Applications Functional Core.

This chapter contains the following topics:

- Introduction to Oracle Fusion Applications Functional Core
- Patching Oracle Fusion Applications Functional Core Database Artifacts
- Patching Oracle Fusion Applications Functional Core Middleware Artifacts
- Log Files
- Monitoring and Troubleshooting Patching Sessions
- Performing System Maintenance Tasks

9.1 Introduction to Oracle Fusion Applications Functional Core

Oracle Fusion Applications Functional Core enables the integration of other Oracle Fusion applications with Oracle Fusion Functional Setup Manager. It provides:.

- APIs and web services to handle the registration of topology objects that are used by the Provisioning software to provision offerings
- The shared libraries required for developing Task Execution Programs for Setup Tasks and Export and Import Services to extend Oracle Fusion Functional Setup Manager content
- APIs and Web services for allowing integration with Oracle Fusion Functional Setup Manager

9.2 Patching Oracle Fusion Applications Functional Core Database Artifacts

The database patches for Applications Functional Core contain Oracle SQL*PLUS scripts. To apply Applications Functional Core database changes, run the SQL*PLUS scripts against the FUSION schema. The patch README file for Applications Functional Core patches contains information to assist you in performing the patching steps correctly.

9.3 Patching Oracle Fusion Applications Functional Core Middleware Artifacts

Oracle Fusion Applications Functional Core uses Oracle ADF Jar files, which may need to be patched.

To patch Oracle Fusion Applications Functional Core middleware artifacts

1. Ensure that the Administration Server, node manager, and database are running.

2. Use the OPatch utility to patch Oracle Fusion Applications Functional Core middleware artifacts. The patch README file for Oracle Fusion Applications Functional Core patches contains information to assist you in performing the patching steps correctly. Follow the steps in Section 7.2, "Patching Applications Core Middleware Artifacts".

3. Stop and start the relevant servers that host the impacted Java EE application.

9.4 Log Files

Oracle Fusion Applications AutoPatch creates log files in the *ATGPF_ORACLE_HOME*/admin/FUSION directory. For more information, see Section 7.3, "Log Files".

9.5 Monitoring and Troubleshooting Patching Sessions

The AD Controller utility, adctrl, can monitor and control the progress of the workers called by Oracle Fusion Applications AutoPatch to update database content. For more information, see Section 7.4, "Monitoring and Troubleshooting Applications Core Patching Sessions".

9.6 Performing System Maintenance Tasks

AD Administration is a standalone utility that performs administration maintenance tasks for the products in *ATGPF_ORACLE_HOME*. The general purpose of the maintenance tasks is to keep your *ATGPF_ORACLE_HOME* files and database objects up-to-date. Some maintenance tasks should be performed systemwide on a regular basis, while others are required infrequently. For more information, see Section 7.5, "Performing System Maintenance Tasks".

10

Performing System Maintenance Tasks

This chapter describes the process of running Oracle Fusion Applications utilities to perform routine system maintenance tasks.

This chapter contains the following topics:

- Introduction to AD Administration
- Maintaining Snapshot Information
- Maintaining Applications Database Entities
- Running Maintenance Tasks Noninteractively
- Running the HomeChecker Utility

10.1 Introduction to AD Administration

AD Administration is a standalone utility that performs administration maintenance tasks for the products in your Oracle Fusion Applications Oracle home and your Applications Core Oracle home. The general purpose of the maintenance tasks is to keep your Oracle Fusion Applications files and database objects up-to-date. Some maintenance tasks should be performed systemwide on a regular basis, while others are required infrequently.

Run AD Administration by using the command-line utility, `adadmin`. This utility has a wrapper script that sets the environment and calls the utility. For UNIX, the wrapper is `adadmin.sh` and for Windows it is `adadmin.cmd`. This brings you to the AD Administration main menu, where you select from a list of submenus that contain these task groups:

- Maintain Snapshot Information
- Maintain Applications Database Entities

After the utility starts, it requires that you enter system information by responding to a series of prompts.

10.1.1 AD Administration Main Menu

The AD Administration main menu is the gateway to submenus, where you select the individual maintenance tasks. For example, selecting **Maintain Snapshot Information** takes you to the Maintain Snapshot Information submenu, where you can run tasks related to snapshots of the application-related files of a given Oracle home.

Figure 10–1   AD Administration Main Menu

```
           AD Administration Main Menu
    -----------------------------------------------

    1.    Maintain snapshot information

    2.    Maintain Applications Database Entities menu

    3.    Exit AD Administration










Enter your choice [3] : []
```

To select a submenu, enter the number of the submenu at the prompt.

10.1.2 Valid Command-Line Arguments

You may want to add arguments to the `adadmin` command to customize its operations. For example, you can add `defaultsfile=defaultsfile_location` to indicate that you want to create a defaults file for use in running maintenance tasks noninteractively, without the need to respond to prompts. For more information, see Section 10.4, "Running Maintenance Tasks Noninteractively".

10.1.3 Prompts and Password Security

When you run AD Administration, it prompts for information about your system. Prompts typically include a description of the information needed, and usually, a default answer is enclosed in brackets. Enter a response to the prompt, or press Enter to accept the default. AD Administration prompts include:

- Confirmation of your Oracle home location

- Log file name

- Batch size

- Confirmation of the correct database

Some submenu options may trigger additional system prompts associated with that task.

For increased security, the `adadmin` command does not prompt for passwords, nor does the program store passwords in clear text or obfuscated format in the restart or defaults file. Instead, it uses the Credential Store Framework (CSF) to store and retrieve passwords from the CSF wallet. For more information, see Section 2.4, "Oracle Fusion Applications Patching and the Security Model".

10.1.4 Starting AD Administration

Follow these steps to start the AD Administration utility:

1. From any directory, start AD Administration with this command, adding any arguments that apply to this session:

    ```
    (UNIX) FA_ORACLE_HOME/lcm/ad/bin/adadmin.sh [argument]
    (Windows) FA_ORACLE_HOME\lcm\ad\bin\adadmin.cmd [argument]
    ```

    AD Administration starts and displays the first prompt.

2. Respond to each prompt by either entering a value or pressing Enter to accept the default value. When you have responded to all of the prompts, the AD Administration main menu appears.

3. Select a menu or submenu option by entering its number in the brackets at the bottom of the screen.

4. From the next menu, select any task by entering its number.

5. You can exit AD Administration from any submenu screen by entering the option number for **Exit AD Administration**.

10.2 Maintaining Snapshot Information

A snapshot represents each unique combination of Oracle home, product, and version at any given point of time. It includes information on each file maintained by Oracle Fusion Applications AutoPatch and a summary of database patches that have been applied to that Oracle home. The information maintained for each file includes the subdirectory where it is located, the name of the file and its version, and the file metadata. The files tracked in the snapshot are those files located in the following `product family` subdirectories: `components`, `db`, and `patch`. Because snapshots track only files for which there can be different versions as shipped by Oracle, they do not track C executable files or log files.

Each time you run Oracle Fusion Applications Patch Manager or Oracle Fusion Applications AutoPatch, the snapshot is updated to include any new file copied to the Oracle home. When you apply a patch, Oracle Fusion Applications Patch Manager performs version-checking against the file to determine which files must be replaced.

The snapshot can be either a current view or a named view.

Current View Snapshot

A **current view** snapshot is a copy of the current file system of the Oracle home. Oracle Fusion Applications Patch Manager creates the current view. The current view is then updated every time a patch is applied and every time the Update Current View Snapshot process runs to maintain a consistent view. Oracle Fusion Applications Patch Manager uses the current view snapshot to determine if all prerequisite patches have been applied to the Oracle home.

For more information, see Section 10.2.1.2, "Update Current View Snapshot".

Named View Snapshot

A **named view** snapshot is a copy of the current view snapshot that you create at a particular time and it is never updated. You can compare one or more named view snapshots to the current view snapshot or refer to previous states of your Oracle home, as needed. Complete file, file version information, and patch history is stored in a named view snapshot.

Properly maintained snapshots allow you to:

- Compare two different Oracle homes

- Compare the same Oracle home at different times

- Track the current status of an Oracle home

Snapshot Tables

Snapshot information is stored in several tables. They contain details such as:

- The name, type, and other attributes of each snapshot

- The list of files, file versions, and other attributes of each file recorded by the snapshot

- The list of patches and bug fixes recorded by the snapshot

Table 10–1 describes the tables related to snapshots.

Table 10–1   Snapshot Tables

Table Name	Description
AD_SNAPSHOTS	Records one entry for each snapshot.
AD_SNAPSHOT_BUGFIXES	Records all patches ever applied at the moment of snapshot creation for a specific snapshot.
AD_SNAPSHOT_FILES	Records all files associated with a particular snapshot.
AD_FILES	Records all files associated with every snapshot in the system. Contains one entry for each file, regardless of how many snapshots and snapshot versions exist. This table may contain files that are no longer in the system to save files for past snapshots.
AD_FILE_VERSIONS	Records all versions for each file that are present in any snapshot.
AD_BUGS	Records all patches that have been applied to the Oracle home.

10.2.1 Maintain Snapshot Information Menu

You can select a task from the Maintain Snapshot Information submenu. Select the last option in the list to return to the AD Administration main menu.

Figure 10–2 Maintain Snapshot Information Menu

```
      Maintain Snapshot Information
      ----------------------------------------

   1.    List snapshots

   2.    Update current view snapshot

   3.    Create named snapshot

   4.    Export snapshot to file

   5.    Import snapshot from file

   6.    Delete named snapshot(s)

   7.    Return to Maintain Applications Files menu




Enter your choice [7] : []
```

10.2.1.1 List Snapshots

This action queries the database and lists all snapshots. It displays the name, type, and comments for each snapshot stored in the AD_SNAPSHOTS table.

10.2.1.2 Update Current View Snapshot

If your current view snapshot is not up-to-date, you can update it. An example of when you may need to run this task is when a snapshot may not have been updated as the result of an interruption during a patching session. All of the other snapshot maintenance tasks are based on the results of this task. You can choose to scan the entire Oracle Fusion Applications Oracle home for all installed product families to determine which component directories should be examined or you can choose a specific product family. For each of those components, it scans these *product family* subdirectories: components, db, and patch. It then updates the database as follows:

■ Inserts and updates the current view snapshot whenever the Update Current View Snapshot runs.

■ Modifies the file and file version information for the current view snapshot.

■ Sets the RAN_SNAPSHOT_FLAG column in the AD_SNAPSHOTS table to Y to indicate that the Update Current View Snapshot ran.

Figure 10–3   Maintain Current View Snapshot

```
Enter your choice [7] : 2


        Maintain Current View Snapshot Information
  ------------------------------------------

  1.    Update all Product Families

  2.    Update a Product Family

  3.    Return to previous Menu




Enter your choice [3] : 2
```

10.2.1.3 Create a Named View Snapshot

This action lists the current view snapshot and prompts you to provide a name. It then performs the following actions:

■   Creates the named view snapshot.

■   Creates a file information list for this snapshot by copying from the current view snapshot.

■   Copies the bug fix list from the current view snapshot.

10.2.1.4 Export a Snapshot to a File

This action lists the snapshots available for export. Then it copies the snapshot file details and snapshot bug fix information to an output file that you specify at the prompt.

10.2.1.5 Import a Snapshot from a File

This action prompts you for the full path and name of the file you want to import. It then updates the snapshot tables with the imported snapshot details.

10.2.1.6 Delete a Named View Snapshot

This action lists the snapshots available for deletion. For the snapshot you select, it deletes the file details and snapshot bug fix entries from the snapshot tables.

10.3 Maintaining Applications Database Entities

Database entities are objects or data related to Oracle Fusion Applications. During standard system use, some database entities may become invalid, for example, through user error or after you apply a large patch. Oracle recommends that you verify the integrity of database entities as a regular maintenance procedure, or whenever the activity of your system indicates that database entities may need revalidation.

AD Administration contains several tasks designed to manage database entities. You access them from the Maintain Applications Database Entities submenu. Some tasks in this menu report on issues, or potential issues, and others actually resolve the issues.

Figure 10–4   Maintain Applications Database Entities

```
        Maintain Applications Database Entities
        --------------------------------------------------

    1.    Compile Invalid Objects

    2.    Health Check

    3.    Re-create grants for FUSION schema

    4.    Maintain multi-lingual tables

    5.    Return to Main Menu




Enter your choice [5] : []
```

10.3.1 Compiling Invalid Objects

As you apply patches and make manual changes to the database, the number of invalid objects can increase. This process compiles invalid database objects in all schemas in the database. As soon as the compile process is complete, AD Administration generates an HTML report that contains information about any objects that remain invalid.

10.3.2 Running the Health Check

The health check process is a centralized set of validity checks that you can perform to ensure that the database is compatible with Oracle Fusion Applications. It validates the schemas and the database objects they contain to verify that they are valid.

The checks performed are as follows:

- Confirms the presence and validity of ADM_DDL in the FUSION_RUNTIME schema

- Identifies grants given to Oracle Fusion Applications and grants given by way of roles. Ensures that no grant is given with the admin option set to Yes. This task grants privileges to roles used by the FUSION_RUNTIME schema.

- Performs various checks on Oracle Fusion Application such as ensuring that synonyms point to valid, existing tables.

- Verifies that privileges are given to roles used by the FUSION_RUNTIME schema.

- Generates a list of invalid objects, compiles the invalid objects, and issues a report that includes the commands to recompile the objects that remain invalid.

The health check process produces a report with its findings, named ad_health_ check_report.html. It also creates two scripts that contain a set of corrective actions that you can take to fix the issues found by the analysis. The scripts may contain steps for you to follow to resolve an issue and they may also contain SQL

actions that are executed when you run the script. The HTML file and both scripts are located in the *FA_ORACLE_HOME* /admin/*SID*/log directory.

The following scripts are created:

- `ad_health_fix_sys.sql`: Run this script as `sysdba`.

- `ad_health_fix_fus.sql`: Run this script as `fusion`.

10.3.3 Recreating Grants and Synonyms

This task grants privileges to roles used by the `FUSION_RUNTIME` schema.

10.3.4 Maintaining Multi-lingual Tables

The standard Oracle Fusion Applications Multilingual Support (MLS) table architecture requires that the multilingual tables (those ending with `_TL`) be fully populated for all active languages. For each row in the base table, there must be a corresponding row in the MLS table for each active language. The Maintain Multilingual Tables utility standardizes and centralizes the synchronization logic for all tables in Oracle Fusion Applications. It relies on the `Application/XDF` dictionary data to know which tables to synchronize and inserts records only when they are missing for a given language. When you install a language, this task automatically runs. You can also run it from the AD Administration menu when you have reason to believe that the data in the `_TL` table is not synchronized. For more information, see Section 6.4, "Install a Language Pack".

10.4 Running Maintenance Tasks Noninteractively

The previous sections have so far described how to run AD Administration interactively - you start the `adadmin` utility and respond to system prompts, select a submenu from the main menu, and then select the task you want to run from that submenu. You can also run AD Administration noninteractively by specifying a defaults file that contains the information necessary to run one of the maintenance tasks. The first time you create the defaults file, you run the `adadmin` command interactively, and then you can reuse the defaults file for the task that you performed.

This section describes the steps necessary to create a defaults file and save it for when you want to run one of the AD Administration tasks without user intervention. You may want to use the noninteractive functionality for long-running tasks, such as compiling the schema.

10.4.1 Creating a Defaults File

To create a defaults file, you add the option `defaultsfile= *defaults file location*` to your `adadmin` command. The following example syntax shows how to create a defaults file for compiling the schemas:

```
(UNIX) FA_ORACLE_HOME/lcm/ad/bin/adadmin.sh defaultsfile=FA_ORACLE_
HOME/admin/$TWO_TASK/default_compile.txt
```

```
(Windows) FA_ORACLE_HOME\lcm\ad\bin\adadmin.cmd defaultsfile=FA_ORACLE_
HOME\admin\%LOCAL%\default_compile.txt
```

The next time you want to perform this same task noninteractively, call the `adadmin` command in noninteractive mode and specify the defaults file. Then run the `adadmin` command interactively to record the history of the session in the specified defaults file.

The following example specifies the defaults file:

```
(UNIX) FA_ORACLE_HOME/lcm/ad/bin/adadmin.sh defaultsfile=FA_ORACLE_
HOME/admin/$TWO_TASK/default_compile.txt interactive=no

(Windows) FA_ORACLE_HOME\lcm\ad\bin\adadmin.cmd defaultsfile=FA_ORACLE_
HOME\admin\%LOCAL%\default_compile.txt interactive=no
```

When you use the defaults file in noninteractive mode, your adadmin session reads the contents of the defaults file to respond to the prompts.

10.4.2 Selecting a Menu Option Noninteractively

You can select a specific AD Administration menu option by specifying the menu name when you call the adadmin command. This functionality allows you to perform specific tasks somewhat noninteractively without using a defaults file. You must respond to the initial adadmin prompts. The following example shows how to run adadmin to compile the schemas:

```
(UNIX) FA_ORACLE_HOME/lcm/ad/bin/adadmin.sh menu_option=CMP_INVALID

(Windows) FA_ORACLE_HOME\lcm\ad\bin\adadmin.cmd menu_option=CMP_INVALID
```

If you select a menu option that contains additional prompts, such as List Snapshots, then you must respond to those prompts interactively. Table 10–2 provides a list of menu names that you can specify with menu_option when running the adadmin command.

Table 10–2   AD Administration Menu Options

Menu Name	Description
LIST-SNAPSHOT	Lists snapshots
UPDATE_CURRENT_VIEW	Updates the current view snapshot
UPDT_PROD_CURR_VIEW	Updates the current view snapshot for a product
CREATE_SNAPSHOT	Creates a named view snapshot
EXPORT_SNAPSHOT	Exports a snapshot to a file
IMPORT_SNAPSHOT	Imports a snapshot from a file
DELETE_SNAPSHOT	Deletes a named view snapshot
CMP_INVALID	Compiles schemas
HEALTH_CHECK	Performs the health check analysis
CREATE_GRANTS	Re-creates grants and synonyms for the FUSION_RUNTIME schema
MAINTAIN_MLS	Maintains multi-lingual tables

10.4.3 Selecting a Menu Option While Using a Defaults File

You can combine the functionality provided by adding menu_option to the adadmin command along with specifying a defaults file. This allows you to bypass responding to prompts interactively. However, if you add the menu_option selection to the adadmin command while referencing an existing defaults file, your session executes only that menu choice from the defaults file. For example, if your defaults file was created to compile schemas and update the current view snapshot, the following command would update only the current view snapshot:

```
(UNIX) FA_ORACLE_HOME/lcm/ad/bin/adadmin.sh menu_option=update_current_view
defaultsfile=FA_ORACLE_HOME/admin/$TWO_TASK/mydefaults.txt

(Windows) FA_ORACLE_HOME\lcm\ad\bin\adadmin.cmd menu_option=update_current_view
defaultsfile=FA_ORACLE_HOME\admin\%LOCAL%\mydefaults.txt
```

10.5 Running the HomeChecker Utility

The HomeChecker utility verifies the correctness of any Oracle Fusion Applications Oracle home directory. It verifies that the duplicated Oracle Applications Development Framework (Oracle ADF) libraries within Oracle Fusion Applications are synchronized with each other. While separate copies of the libraries are maintained, they are treated logically as a unit and this utility verifies that the libraries are still consistent with each other. HomeChecker also ensures that the artifacts within the Oracle home match the central Oracle Inventory, to confirm that the artifacts were laid down either as part of the initial installation or by a subsequent patch. For more information, see Section 2.1.5, "Oracle Universal Installer (OUI) Inventory".

The HomeChecker output displays the following information:

- Libraries that are not synchronized

- Oracle Fusion Applications artifacts that are not synchronized

- Libraries that are synchronized

- Oracle Fusion Applications artifacts that are synchronized

You would most likely run the HomeChecker utility when you are working with Oracle Support Services to diagnose issues with your environment.

To run the HomeChecker utility

Run the following command:

```
(UNIX) FA_ORACLE_HOME/lcm/ad/bin/homechecker.sh -validate FA_ORACLE_HOME path
[-logfile log file name] [-prodfamily comma-separated list of product families]
[-reportfile
report file path] [-loglevel log level]

(Windows) FA_ORACLE_HOME\lcm\ad\bin\homechecker.cmd -validate FA_ORACLE_HOME path
[-logfile log file name] [-prodfamily comma-separated list of product families]
[-reportfile
report file path] [-loglevel log level]
```

Table 10–3 HomeChecker utility parameters

Parameter	Description	Mandatory
validate	Specify the path to FA_ORACLE_HOME	Yes
logfile	Overrides the default log file name and sends the processing information to the file you specify, under the FA_ORACLE_HOME/admin/FUSION/log directory	No
prodfamily	Supply a comma-separated list of product families you want to see on the report	No
reportfile	Supply the directory path and file name for report output	No, the default is the current directory

Table 10–3   (Cont.) HomeChecker utility parameters

Parameter	Description	Mandatory
loglevel	Records messages in the log file at the level you specify. Enter a value to override the default log level of `INFO`. See Section 11.1, "Oracle Fusion Applications Patch Manager Logging".	No

11

Monitoring and Troubleshooting Patches

This chapter describes how to monitor and troubleshoot Oracle Fusion Applications patching and AD Administration processing sessions.

This chapter contains the following topics:

- Oracle Fusion Applications Patch Manager Logging
- Monitoring Patching Sessions
- General Troubleshooting for Oracle Fusion Applications Patching
- Troubleshooting Patching Sessions for SOA Composites
- Troubleshooting Patching Sessions for Database Content

11.1 Oracle Fusion Applications Patch Manager Logging

Oracle Fusion Applications Patch Manager creates log files for the actions it performs. These logging capabilities track the progress of actions and assist you in diagnosing issues. When you use Oracle Fusion Applications Patch Manager, you can specify the level of logging detail. The following log levels are available:

- ERROR:1 (SEVERE) For an error that results in a failure.
- WARNING:1 (WARNING) For an error that does not result in failure but that you should review.
- NOTIFICATION:1 (INFO) For high-level information about the progress of the process, no action necessary.
- NOTIFICATION:16 (CONFIG) For more detailed information about the progress of the process, no action necessary
- TRACE:1 (FINE) For generating the first level of trace messages, used for diagnosing issues.
- TRACE:16 (FINER) For generating the second level of trace messages, used for diagnosing issues.
- TRACE:32 (FINEST) For generating the highest level of trace messages, used for diagnosing issues.

When you select a more detailed level of logging, the log files also include the lower level of details. For example, if you choose to see INFO messages in your log file, WARNING and SEVERE messages also appear in the log files. For more information, see "Standard Logging Levels" in the *Oracle Fusion Applications Administrator's Guide*.

11.1.1 Log Files for Patching Sessions

You can examine the activities performed during patching sessions by reviewing the associated log files. Oracle Fusion Applications Patch Manager consolidates log files for each patching session under the directory, *FA_ORACLE_HOME*/admin/FUSION/log. This directory contains the top-level log file, logsummary_*fapmgr_command_timestamp*.html, along with related log files for each task performed during a fapmgr session. During a session, you can view the Log Summary HTML file from a browser, which provides links to individual log files. You can periodically refresh the Log Summary HTML file to view the progress of the current patching session. If a task fails, you can access the links to the associated log files to assist in diagnosing the failure. For more information, see Section 11.2.1, "Log Summary".

When a new session starts, the log files from the previous session move to *FA_ORACLE_HOME*/admin/FUSION/logarchive/*Patch Number*/*fapmgr_command*/*session ID*/*timestamp*. The session ID is unique and the time stamp is the start time for the session. Note that whenever Oracle Fusion Applications Patch Manager runs a command where there is no patch number, such as bootstrap, abort, and report, the archive logs are named *FA_ORACLE_HOME*/admin/FUSION/logarchive/fapmgr_command/*timestamp*.

Log files for OPatch actions are initially written to the *FA_ORACLE_HOME*/cfgtools/opatch/*patch number_timestamp* directory.

Table 11–1 contains a list of log files created by Oracle Fusion Applications Patch Manager during patching activities.

Table 11–1   Log Files for Patching Activities

Log file name under FA_ORACLE_HOME/admin/FUSION/log	Log file generated from...
FAPatchManager_apply_*timestamp*.log	Oracle Fusion Applications Patch Manager apply session
FAPatchManager_abort_*timestamp*.log	Oracle Fusion Applications Patch Manager abort session
FAPatchManager_bootstrap_*timestamp*.log	Oracle Fusion Applications Patch Manager bootstrap session
FAPatchManager_report_*reportname_timestamp*.log	Oracle Fusion Applications Patch Manager report session
FAPatchManager_validate_*timestamp*.log	Oracle Fusion Applications Patch Manager validate session
adpatch_apply_*timestamp*.log	Oracle Fusion Applications AutoPatch apply session
adpatch_abort_*timestamp*.log	Oracle Fusion Applications AutoPatch abort session
adpatch_apply_*timestamp*_worker*number*.log	Oracle Fusion Applications AutoPatch worker log file
adpatch_validate_*timestamp*.log	Oracle Fusion Applications AutoPatch
adpatch_apply_*timestamp*_timingreport.lst	Oracle Fusion Applications AutoPatch timing report
logsummary_*fapmgr_command_timestamp*.html For reports: logsummary_report_*reportname_timestamp*.html	The consolidation of the log files generated by Oracle Fusion Applications Patch Manager in HTML format for viewing and accessing links to other log files from a browser
patch number_fapmgr_command_session id_timestamp.marker	Marker file used while moving log files to a backup directory

Table 11–1   (Cont.) Log Files for Patching Activities

Log file name under FA_ORACLE_ HOME/admin/FUSION/log	Log file generated from...
ConfigContext_*timestamp*.log	Oracle Fusion Applications Patch Manager in online mode
ExecutionContext_*timestamp*.log	Oracle Fusion Applications Patch Manager in online mode
FAPMgrDiagnosticsSummary*fapmgr_command_ timestamp*.html	The consolidation of the Oracle Fusion Applications Patch Manager session in HTML format, known as the Diagnostics report
FAPMgrDiagnosticsSummary.html	The Diagnostic report when it is run on demand using this command syntax: fapmgr.sh report -patchprogress. For more information, see Section 3.5.5.1, "Running the Diagnostics Report".

11.1.2 Timing Reports

For information about the duration of patching tasks, refer to the Diagnostics Report, in Section 11.2.2, "Diagnostics Report".

11.2 Monitoring Patching Sessions

Oracle Fusion Applications Patch Manager coordinates patching activities by assigning tasks based on information from the patch metadata file. OPatch runs the tasks for updating middleware artifacts and Oracle Fusion Applications AutoPatch runs the database tasks. Each of these tools generates one or more log files containing informational and error messages generated during patching. For more information, see Section 11.1.1, "Log Files for Patching Sessions". If a task fails, the exact failure information for a given task is included in the log file. You can view the progress of the patching session from a browser, including the details of a failed task, by reviewing the Log Summary.

11.2.1 Log Summary

The Log Summary is created automatically whenever you start an Oracle Fusion Applications Patch Manager session. The Log Summary is continuously updated as the session progresses. This report exists in the *FA_ORACLE_ HOME*/admin/FUSION/log directory and is named logsummary_*fapmgr_ command_timestamp*.html. It contains links to all of the log files generated during the session. To view the report, open the report from your browser and periodically refresh the page to see updated links to log files as they are created. You can open those links and monitor the progress of the session by refreshing the browser.

11.2.2 Diagnostics Report

After each patching sessions ends, the Diagnostics report is automatically generated so that you can view the results of the session from a browser. You can also use this report during a patching session that is currently running, by generating the report from the command line. The Diagnostics report is located in the *FA_ORACLE_ HOME*/admin/FUSION/log directory and is named FAPMgrDiagnosticsSummary*fapmgr_command_timestamp*.html. For more information, see Section 3.5.5, "Diagnostics Report".

11.3 General Troubleshooting for Oracle Fusion Applications Patching

This section contains the following general troubleshooting scenarios for patching:

- Starting a New Patching Session After the Previous Session Failed
- Abandoning a Failed Patching Session
- Recovering from an Interrupted Patching Session
- Retrying Failed Post-Patching Tasks in a Previous Session
- Avoiding a Lost Connection During the Patching Session
- Resolving Components Locked by a Singleton Patch
- Resolving a Webcat Patch File Creation Failure
- Resolving an EditTimedOutException Error
- Finding Artifact Versions
- Backing Out Patches After They Have Been Successfully Applied

For troubleshooting information that is specific to patching security artifacts such as the `jazn-data.xml` file, data security files, and data role templates, see Section 4.17, "Patching Security Artifacts". For troubleshooting information that is specific to patching SOA composites, see Section 11.4, "Troubleshooting Patching Sessions for SOA Composites". For troubleshooting information that is specific to patching database content, see Section 11.5, "Troubleshooting Patching Sessions for Database Content".

11.3.1 Starting a New Patching Session After the Previous Session Failed

The previous patching session failed, and when you attempt to start a new patching session, a message appears about a previous session having failed.

The previous patching session could be in various states after its failure. The following scenarios are possible:

- To abandon the previous session and start a new session, see Section 11.3.2, "Abandoning a Failed Patching Session".

- In some cases, the patch tables do not correctly reflect the failed state of the patching session and may still show a patch task as running. In this case, you must use the `forcefail` command to fail the session. Then you can abandon the current patching session. For more information, see Section 11.3.3, "Recovering from an Interrupted Patching Session".

- There can be only one patching session active at one time for Oracle Fusion Applications, Oracle Fusion Functional Setup Manager, and Oracle Fusion Middleware Extensions for Applications (Applications Core). If there is a failed Applications Core or Functional Setup Manager patching session that needs to be cleaned up, see Section 7.4.6, "Abandoning a Failed Patching Session".

11.3.2 Abandoning a Failed Patching Session

The previous patching session failed and you want to start a new patching session. Only one patching session can be running at a time.

Always make sure that processes associated with the previous patching session do not exist. You can abandon a previously failed session by running the `fapmgr abort` command so that you can start a new patching session. The `abort` command cleans up any intermediate states tracked by `fapmgr` and moves the log files for the

abandoned session to an archive log directory. You cannot abandon a session that is actively running.

Use the following syntax for the `fapmgr abort` command:

```
(UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh abort [-logfile log file name]
[-loglevel level]
(Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd abort [-logfile log file name]
[-loglevel level]
```

Table 11–2 describes the options available for the `abort` command.

Table 11–2   abort Command Options

Option	Description	Mandatory
logfile	Name of the log file.	No, default value is FAPatchManager_abort_*timestamp*.log
loglevel	Reporting level for messages. See Section 11.1, "Oracle Fusion Applications Patch Manager Logging".	No, default value is INFO
help	Displays help.	No

If the `fapmgr abort` command errors with a message, such as, "Another APPLY session is already running", you may need to use the `fapmgr forcefail` command first. For more information, see Section 11.3.3, "Recovering from an Interrupted Patching Session". Also confirm that the table FND_INSTALL_PROCESSES does not exist.

11.3.3 Recovering from an Interrupted Patching Session

The patching session was interrupted by a system failure when Oracle Fusion Applications Patch Manager and Oracle Fusion Applications AutoPatch were running. The patching-related database tables still show the patching session as running, but no patching-related processes are actually running.

Use the `fapmgr forcefail` command to update the patching tables. Confirm that no patching processes are running before you use this command.

1. Confirm that all processes related to this patching session are no longer active. From your operating system, check for processes that are running `fapmgr`, `javaworker`, `adpatch`, `adadmin`, and `adworker`. If any processes are running, you must stop them using the command appropriate for your operating system.

2. Use the `fapmgr forcefail` command to update the patching tables.

    ```
    (UNIX) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh forcefail [-logfile log file name]
    [-loglevel level]

    (Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.cmd forcefail [-logfile log file
    name] [-loglevel level]
    ```

3. From this point you can either abandon or restart the failed session.

    ■ To abandon the failed patching session, follow the steps in Section 11.3.2, "Abandoning a Failed Patching Session".

    ■ To restart the failed patching session, use the `fapmgr apply` command to apply the same patch. The session starts from the failed task.

> **Note:** Oracle Fusion Applications Patch Manager, Functional Setup Manager, and Applications Core all use Oracle Fusion Applications AutoPatch for database patching. If a patching session is hung or incomplete, you may potentially need to consider the impact of an Applications Core or Functional Setup Manager patching session. Only one patching session can be active at a time.

11.3.4 Retrying Failed Post-Patching Tasks in a Previous Session

When you apply patches in online mode using the `stoponerror` option and post-patching tasks fail, you can use the `fapmgr retry` command. The `retry` mode of `fapmgr` lets you attempt all failed online post-patching operations for a specific patching session. These actions include not only the restart of Managed Servers, but also automated actions for other artifacts, such as deployment of SOA composites, Oracle BPM templates, and IPM artifacts. If you do not use the `fapmgr retry` command, you must manually perform the post-patching operations that failed.

11.3.4.1 Requirements for retry mode

The following conditions must be met for `retry` mode to work:

1. The session_id must exist in the database. To verify this, this SQL*Plus query should return one row:

   ```
   select count(*) from ad_patch_util_sessions where session_id=session_id;
   ```

2. The failed session must have at least one failed life cycle operation.

3. The patch top directory from the original session must exist.

4. You must have followed these steps when you originally applied the patch:

   a. Run `fapmgr validate -online`.

   b. Fix the infrastructure failures reported by validation.

   c. Run `fapmgr apply -online -stoponerror`

   If you did not resolve the infrastructure failures reported by patch validation, the retry will most likely fail.

11.3.4.2 Running fapmgr in retry mode

When you run fapmgr in `retry` mode, the same command line options that were used in the original session are used. Use the following command syntax:

```
(Unix) FA_ORACLE_HOME/lcm/ad/bin/fapmgr.sh retry -sessionid [-logfile log_file_
name]
 -loglevel log_file_name] [-loglevel level]
(Windows) FA_ORACLE_HOME\lcm\ad\bin\fapmgr.sh retry -sessionid [-logfile log_file_
name]
 -loglevel log_file_name] [-loglevel level]
```

For the retry session, `fapmgr` uses the same session_id, but the timestamp is different. The log files for the apply session and the retry session are created in different directories, and the sessions create two separate Diagnostics reports.

11.3.5 Avoiding a Lost Connection During the Patching Session

If you initiate a patching session from a terminal server, such as a laptop, you may lose the connection during extended periods of time when no messages are sent to the terminal. The terminal server may interpret this as inactivity and then end the session. For example, no messages are sent to the client when Oracle Fusion Applications Patch Manager is stopping and starting servers, waiting for a failed task to be fixed, or is hung on a database task. To avoid this situation, ensure that the terminal server is configured appropriately to handle long durations of inactivity.

11.3.6 Resolving Components Locked by a Singleton Patch

If you recently applied a one-off patch to a middleware artifact, you may encounter the following error the next time you apply a standard patch:

```
The incoming patch(es) [patch_number] target components that are locked by
singleton patch(es) [patch_number].
OPatch cannot proceed. Please refer to log file for more details.
```

A one-off middleware patch sets a lock on the component that the one-off patch updates. After you apply a one-off patch, you must subsequently apply the related standard patch that contains the same updates as the one-off to release the lock. The error message tells you which one-off patch is locking the component. For more information, see Section 2.2.1, "Impact of a One-off Patch".

> **Note:** OPatch uses the term *singleton* patch, which is equivalent to a *one-off* patch, as used by Oracle Fusion Applications Patch Manager.

11.3.7 Resolving a Webcat Patch File Creation Failure

If you apply a patch that contains BI Publisher artifacts, the BI Presentation servers should not be running. The following error occurs if the BI Presentation servers are running during the deployment of BI Publisher artifacts:

```
java.lang.RuntimeException: Webcat patch file creation failed!
```

To resolve this issue, shut down the BI Presentation servers to release locks on the Oracle BI Presentation Catalog. For more information, see "fastartstop Syntax" in the *Oracle Fusion Applications Administrator's Guide*.

11.3.8 Resolving an EditTimedOutException Error

If you receive the following error during patch validation,

```
weblogic.management.mbeanservers.edit.EditTimedOutException
```

you may have to manually release the edit session. This situation can occur when a domain is already in "edit" mode during patching, such as when the server crashes when Oracle Fusion Applications Patch Manager tries to stop and restart it.

Follow these steps to manually release the edit session:

1. Log in to the admin console for the domain that is locked in edit mode.

2. In the admin console, confirm that **Release Configuration** is enabled in the **Change Center** menu.

3. Click **Release Configuration** to release the edit session.

11.3.9 Revert To a Previous Flexfield Definition After It Is Updated By a Patch

After you apply a patch that contains flexfield changes and you decide you are not ready to implement those flexfield changes, you have the option to revert to a previous version of that flexfield definition. The Flex Modeler creates an MDS label, `FlexPatchingWatermark`*date+time*, before it initiates the flexfield deployment, which establishes the watermark for what was in MDS before the patch was applied. For your reference, the name of the label is included along with the Flex Deployment report in the patching log file. To use a previous version of a flexfield definition, use the WLST command `promoteMetadataLabel`. For more information, see "promoteMetadataLabel" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

To delete all previous MDS labels for a flexfield, after you confirm that you can use the changes delivered by a patch, use the WLST command `deleteFlexPatchingLabels`. Note that keeping old MDS labels adversely impacts performance. For more information, see "Using the WLST Flexfield Commands" in the *Oracle Fusion Applications Developer's Guide*.

11.3.10 Resolving an Online Validation Error for BI Artifacts

If a patch contains BI artifacts the BI OPMN control process, which is similar to a node manager, has to be up for online mode validation to succeed. Online validation reports the following error if the BI OPMN control process is not up:

```
The deployment of BI Publisher artifacts will not be attempted because the
BI Presentation server is neither fully started nor down.
One likely cause is that the BI OPMN control process is not running. Make
sure that the BI OPMN control process is up and the BI
Presentation server is started successfully before applying this patch. If
this server is not fully started, you must stop the BI Presentation
server, manually deploy the BI Publisher artifacts, and then re-start the BI
Presentation server
```

To resolve the issue, you must ensure that the BI OPMN control process is up and running.

11.3.11 Finding Artifact Versions

The `Opatch -lsinventory -detail` command provides a report that lists all patches, artifacts and artifact versions that were modified within each patch applied to a given Oracle home. This report lists only artifacts that were modified. If an artifact does not appear on this report, then the artifact remains at its base version. Run this report when you are working with Oracle Support Services and you need to provide an artifact version.

Use this command syntax to generate the report:

```
OPatch/opatch lsinventory -detail -oh FA_ORACLE_HOME -invPtrLoc \
FA_ORACLE_HOME/oraInst.loc -jre JAVA_HOME
```

The following example depicts the section of the report that displays patches applied. To use the report, you must find the latest entry for the specific artifact and note the version reported.

```
Interim patches (11) :

Patch  11801        : applied on Wed Feb 02 17:57:53 PST 2011
   Created on 18 Jan 2011, 16:09:54 hrs PST8PDT
   Bugs fixed:
```

```
    11801
  Patch is translatable.
  Files Touched:
    AdfPjfIntMspUi.jar, version "23.0" --> ORACLE_
HOME/prj/deploy/EARProjectsFinancials.ear/EARProjectsFinancials.war/WEB-INF/lib/Ad
fPjfIntMspUi.jar
  Patch Location in Inventory:
    /u01/FUSIONAPPS_APPLTOP/fusionapps/applications/inventory/oneoffs/11801
  Patch Location in Storage area:
    /u01/FUSIONAPPS_APPLTOP/fusionapps/applications/.patch_storage/11801_Jan_18_
2011_16_09_54

Patch  12801        : applied on Tue Feb 01 21:30:17 PST 2011
  Created on 28 Jan 2011, 14:26:56 hrs PST8PDT
  Bugs fixed:
    12801
  Patch is translatable.
  Files Touched:
    EFFmetadata.mar, version "35.0" --> ORACLE_
HOME/hcm/deploy/EarHcmCoreSetup.ear/EFFmetadata.mar
    system-jazn-data.xml, version "35.0" --> ORACLE_
HOME/hcm/security/policies/system-jazn-data.xml
  Patch Location in Inventory:
    /u01/FUSIONAPPS_APPLTOP/fusionapps/applications/inventory/oneoffs/12801
  Patch Location in Storage area:
    /u01/FUSIONAPPS_APPLTOP/fusionapps/applications/.patch_storage/12801_Jan_28_
2011_14_26_56
```

For more information about OPatch, see the *Oracle Fusion Middleware Patching Guide*.

11.3.12 Backing Out Patches After They Have Been Successfully Applied

You should always test the application of a patch and the functionality related to the patch on a test system. After the patch is successfully tested, apply the patch on the production system. There is no automated method of backing out patches. Oracle strongly recommends that you work with Oracle Support Services if you must back out a patch.

11.4 Troubleshooting Patching Sessions for SOA Composites

The information provided in this section describes the troubleshooting process for errors that can occur when patching Service-Oriented Architecture (SOA) composites. These processes assume that you validate the patch and then apply the patch in online mode. SOA patching errors can be divided into the following categories:

- **Error occurs during validation**

  Oracle Fusion Applications Patch Manager can detect and report validation errors before changes have occurred to the file system. If you do not resolve validation errors before applying the patch, the patch fails and you must manually deploy the SOA composites after you resolve the validation errors.

- **Error occurs during the patch apply phase**

  These errors may require contacting Oracle Support Services to restore the system back to a known working state and can be further divided into these categories:

  - The SOA composite failed to deploy and Oracle Fusion Applications Patch Manager recovered from the failure.

- The SOA composite was not deployed successfully and the recovery failed. Therefore, the composite may be partially deployed.

- The system is in an unknown state, as the result of a timeout occurring during deployment. Oracle Fusion Applications Patch Manager cannot determine if the SOA composite is deployed, not deployed, or partially deployed.

When SOA composite failures occur, review the error messages in the Diagnostics report and related log files and follow the applicable steps in one or more of the following categories:

- Basic Troubleshooting for SOA Composite Failures

- Troubleshooting SOA Composite Validation Failures

- Troubleshooting SOA Composite Deployment Failures

- Troubleshooting Complex Failures during SOA Patching

11.4.1 Basic Troubleshooting for SOA Composite Failures

SOA composite validation and deployment can fail for multiple reasons. Review the following steps for basic troubleshooting:

1. After you validate or apply a patch that contains SOA composites, review the Diagnostics report for errors.

   Oracle Fusion Applications Patch Manager generates the Diagnostics report after every validation and patching session. The report output is in HTML format for viewing from a browser and is located here: *FA_ORACLE_HOME*/admin/FUSION/log/FAPMgrDiagnosticsSummary*date:session*.html.

   The **Module Task Details** section of report displays the following information to assist in your troubleshooting:

   - Mode: Middleware, in this case.

   - Phase: Validation or Patch Application, in this case.

   - Product Family: The short name of the product family.

   - Task: The following information displays for SOA composites:
     - Name of composite
     - Domain name
     - Path to composite JAR in *FA_ORACLE_HOME*
     - Revision of composite

   - Status: Possible values of Success, Failed, or Skipped.

   - Duration: Total time the task ran.

   - Start Time: Time and date the task started.

   - End Time: Time and date the task ended.

   - Warning/Error Message: The error message displays as a `java.lang.RuntimeException`. The message often includes a suggestion for resolving the failure.

   - Log file: The path and file name of the high level log file, `FAPatchManager_fapmgr_command_timestamp`.log, associated with the task. From the Module Execution Summary section of the Diagnostics report, you can review

log files by accessing the link to the Log Summary. For more information, see Section 11.2.1, "Log Summary".

- Line Numbers: The line numbers in the log file associated with the task.

2. SOA log files are located in this directory: `FA_ORACLE_HOME`/admin/FUSION/log/fapatch/fapatch_`release_number`/soalogs. If merge operations are performed on a SOA composite, due to runtime customizations, such as design time and run-time (DT@RT) changes or property changes, a merge log file is generated. There is one merge log file per domain and the name of merge log files follows this naming convention: `fapatch_domain_nametimestamp`.merge.log

3. Restart the SOA servers and for each failure, follow Steps 4 through 9.

4. Determine if there is a cause for the error that needs to be resolved, in addition to restarting the server, by referring to the Diagnostics report, Oracle Fusion Applications log files and SOA log files. Examples of other causes include database errors, coherence configuration errors, and out of memory issues. For more information, see "Troubleshooting Oracle SOA Suite" in the *Oracle Fusion Applications Troubleshooting Guide*.

5. Determine if you need to manually restore the system back to its state before the application of the patch was attempted. The following scenarios do not require manual restoration of the system:

- Errors occurred during the validation phase.

- Errors occurred during the patch application phase but the recovery was successful, so the system was recovered to its original state. The Diagnostics report displays this condition in this message:

  ```
  Deployment of SOA composite[artifact_name and path]failed, but the system
  has recovered successfully.
  Suggestion: You must manually deploy the composite using the WLST command.
  ```

  If you need to restore the system, follow the steps in Step 6.

6. If a failed deployment leaves a composite in an inconsistent state, you must restore the system to its original state. Follow these steps to use WLST commands to restore the system. If you prefer to use Oracle Fusion Applications Control to restore the system, see Step 7.

   a. Find out what the active revision of the composite was before the application of the patch from the Diagnostics report, as indicated by this message: `The last active version of the composite before patch application began was [version]`.

      In the following examples, 1.0 is the previous revision and 2.0 is the patched revision.

   b. Undeploy the patched revision of the composite if it exists in the system.

      ```
      sca_undeployComposite('http://server01:8001', 'POProcessing', '2.0')
      ```

   c. Mark the previously active revision of the composite as active and as a default revision.

      To activate the old revision:

      ```
      sca_activateCompositeMb('POProcessing', '1.0')
      ```

      To assign the default composite:

```
sca_assignDefaultCompositeMb('POProcessing', '1.0')
```

7. Follow these steps to restore the system to its original state using Oracle Fusion Applications Control.

   a. Find the active revision of the composite before the application of the patch from the Diagnostics report, as indicated by this message: `The last active version of the composite before patch application began was [version]`.

      In the following example, 1.0 is the previous revision and 2.0 is the patched revision.

   b. Undeploy the patched revision of the composite if it exists in the system. For more information, see "Undeploying Applications" in the *Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite and Oracle Business Process Management Suite*.

   c. Mark the previously active revision of the composite as active and as a default revision. For more information, see "Managing the State of All Applications at the SOA Infrastructure Level" in the *Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite and Oracle Business Process Management Suite*.

8. Manually deploy the SOA composites included in the patch by following the steps in Section 4.18.2, "Manually Deploying SOA Composites".

9. If you are unable to resolve the failure, file a service request with Oracle Support Services and provide the logs and information as described in "Table 9-2 SOA Log Information for Oracle Support Services" in the *Oracle Fusion Applications Troubleshooting Guide*.

11.4.2 Troubleshooting SOA Composite Validation Failures

This section describes common problems and solutions for SOA composite validation failures. Errors that occur during the validation phase must be resolved before applying the patch. If you encounter these errors during patch application, you must manually deploy the SOA composites after you resolve the validation errors. Oracle Fusion Applications Patch Manager captures the OPatch validation log files, which can be found by referencing the Diagnostics report or the Log Summary. The errors in the log files provide information about the cause of the failure and are often followed by recommended actions.

This section contains troubleshooting information about the following failures:

- Oracle JDeveloper Customization Error

- SOA Server Not Available

- Administration Server Not Available

- SOA-Infra Server Is Ready

- Composite with Identical Revision Is Already Deployed

11.4.2.1 Oracle JDeveloper Customization Error

An error that is related to a JDeveloper customizations occurs when you customized a SOA composite and did not save the customizations. You must save these customizations before you apply a patch that includes the next revision of the composite. Follow the steps in Section 4.18.1, "Preserving SOA Composite JDeveloper Customizations Before Applying a Patch" to resolve this error.

11.4.2.2 SOA Server Not Available

If the SOA server is down or not available for patching, patch validation succeeds, but you receive a warning message stating that the deployment of the composite will not be performed because the SOA infrastructure is down.

Use Oracle Enterprise Manager Fusion Applications Control (Fusion Applications Control) to check the state of the SOA server. For example, if an "Initializing SOA" warning message displays on the home page, Oracle recommends that you wait until the SOA server is completely up and running, with all composites initialized.

For more information, see "SOA Server Does Not Start" in the *Oracle Fusion Applications Troubleshooting Guide*.

11.4.2.3 Administration Server Not Available

If the Administration Server is down or not available for patching, patch validation fails. Use Fusion Applications Control to check the state of the Administration Server.

11.4.2.4 SOA-Infra Server Is Ready

If the SOA-infra server is down or not available for patching, patch validation fails.

Use Fusion Applications Control to check the state of the SOA-infra server. Confirm that all dependent services are running and that all composites deployed into the SOA-infra server are present. It may take some time after SOA-infra is up for all services to initialize. If you are using a cluster, you must perform this check for all SOA-infra servers in the cluster.

11.4.2.5 Composite with Identical Revision Is Already Deployed

If you receive an error stating that a composite with a specific revision is already deployed, the SOA composite in the patch was previously deployed by a patch or manually by a user.

You can resolve this error either by not applying the current patch or by undeploying the composite before applying the patch. Note that if you undeploy the composite, you lose any customizations you may have made to that composite. Use the following command to undeploy a composite.

```
sca_undeployComposite('server_URL', 'composite_name', 'composite_revision')
```

11.4.3 Troubleshooting SOA Composite Deployment Failures

This section describes common problems and solutions for SOA composite deployment failures during patching. Errors that occur during the deployment phase must be resolved as soon as possible because the system has been modified. Do not try to roll back or reapply patches that have errors during deployment. After you resolve the cause of the error, you must deploy the composite manually.

This section contains the following topics:

- Failed to Make New Composite Revision the Default
- Failed to Retire Previous Composite Revision
- Custom Metadata and Key Flexfield Changes Are Not Propagated Across Clusters

11.4.3.1 Failed to Make New Composite Revision the Default

If you receive an error in making the new composite the default, you can manually assign the new composite as the default.

Use the following WLST command to assign the new composite as the default:

```
sca_assignDefaultComposite('host', 'soaport', 'user', 'password', 'composite_
name', 'composite_revision')
```

If the WLST command is successful, check to see if the new composite is active. If it is not, you must then manually deploy the composite that failed, by following the steps in Section 4.18.2, "Manually Deploying SOA Composites".

For more information, see "sca_assignDefaultComposite" in the Oracle Fusion Middleware WebLogic Scripting Tool Command Reference.

11.4.3.2 Failed to Retire Previous Composite Revision

If you receive an error in retiring the previous version of the composite, the old composite was not retired and both the new and old composites may be running. The old SOA composite was supposed to be retired so that only the new SOA composite would be active.

To resolve this error, use the following Oracle WebLogic Scripting Tool (WLST) command to retire the old composite:

```
sca_retireComposite('host', 'soaport', 'user', 'password', 'composite_name',
'composite_revision')
```

If the WLST command is successful, check to see if the new composite is active. If it is not, you must then manually deploy the composite that failed, by following the steps in Section 4.18.2, "Manually Deploying SOA Composites".

For more information, see "sca_retireComposite" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

11.4.3.3 Custom Metadata and Key Flexfield Changes Are Not Propagated Across Clusters

Custom metadata and key flexfield changes are not propagated across clusters after applying a patch.

Each SOA cluster maintains its own SOA MDS schema, which results in a duplicate set of metadata for each SOA cluster that must be synchronized. Oracle Fusion Applications Patch Manager manages this synchronization, but any custom metadata or flexfield metadata must be manually exported from a source system and then migrated to the other systems. To analyze, export, and import the metadata, follow the steps in "Task: Synchronizing Customized Flexfields in the SOA MDS Repository" in the *Oracle Fusion Applications Extensibility Guide*.

11.4.4 Troubleshooting Complex Failures during SOA Patching

The following failures may require contacting Oracle Support Services. If you are unable to resolve the failure after following the steps in Section 11.4.1, "Basic Troubleshooting for SOA Composite Failures", file a service request with Oracle Support Services and provide the logs and information as described in "Table 22-2 SOA Log Information for Oracle Support Services" in the *Oracle Fusion Applications Administrator's Guide*.

11.4.4.1 No Base Composite Has Been Deployed

An earlier revision of the SOA composite, which is being patched, is not currently deployed in the system. This could mean that the composite was not previously

provisioned on the system. As a result, the patch validation reports the following error:

```
The base composite is not set as default composite. Suggestion: You must manually
set the base composite as the default composite using the WLST command.
```

11.4.4.2 Failure at Preparation Step

The SOA composite fails during export actions, extract or attach plans, or merge updates, causing patch validation to the report the following error:

```
Deployment of SOA composite [{0}] failed at preparation step. Reason: [{1}]
Suggestion: You must manually deploy the composite using the WLST command.
```

11.4.4.3 Unknown Deployment Status

The deployment of the composite reported an unknown deployment status, as shown by the following example message:

```
No information is available about the recovery status. The RecoverStatus object
obtained is null.
```

11.5 Troubleshooting Patching Sessions for Database Content

The AD Controller utility, `adctrl`, can monitor and control the progress of the workers called by Oracle Fusion Applications AutoPatch to update database content and by AD Administration. With AD Controller, you can determine the status of the workers and control their actions. For more information about workers, see Section 3.1.2.1, "Worker Processes".

The following sections contain steps for troubleshooting issues that may occur during patching sessions for database content:

- Starting AD Controller
- Reviewing Worker Status
- Determining Why a Worker Failed
- Restarting a Failed Worker
- Terminating a Hung Worker Process
- Shutting Down the Manager
- Reactivating the Manager
- Resolving the Error, "Unable to start universal connection pool"
- Resolving a Worker Blocked by a Session
- Resolving an Error During Conflict Checking
- Setting the Environment for Troubleshooting Database Issues

11.5.1 Starting AD Controller

Follow these steps to start AD Controller:

1. Start AD Controller with the `adctrl` command.

   ```
   (UNIX) FA_ORACLE_HOME/lcm/ad/bin/adctrl.sh
   (Windows) FA_ORACLE_HOME\lcm\ad\bin\adctrl.cmd
   ```

It prompts you to:

- Confirm the value of the Oracle Fusion Applications Oracle home

- Specify an AD Controller log file. This log file is written to the current working directory. The default is `adctrl.log`.

2. After the main menu displays, enter a number to select an option. You can press Enter at any time to return to the AD Controller main menu.

```
                    AD Controller Menu
        ------------------------------------------------

    1.    Show worker status

    2.    Tell worker to restart a failed job

    3.    Tell worker to quit

    4.    Tell manager that a worker failed its job

    5.    Tell manager that a worker acknowledges quit

    6.    Restart a worker on the current machine

    7.    Exit




Enter your choice [1] : []
```

11.5.2 Reviewing Worker Status

When Oracle Fusion Applications AutoPatch or AD Administration runs tasks in parallel, it assigns tasks to workers for completion. There may be situations that cause a worker to stop processing. You can use AD Controller to determine the status of workers and manage worker actions. You can also find the status of workers by reviewing the Log Summary. For more information, see Section 11.2.1, "Log Summary".

Follow these steps to review the status of the workers from AD Controller:

1. Start AD Controller. For more information, see Section 11.5.1, "Starting AD Controller".

2. Review worker status.

   Select **Show worker status** from the AD Controller main menu. AD Controller displays a summary of current worker activity. The summary columns are:

   - Control Code: The last instruction from the manager to the worker

   - Worker: The worker number

   - Context: The general action the manager is executing

   - Filename: The file the worker is running, if any

   - Status: The status of the worker

     Table 11–3 describes the status that may be assigned to a worker.

Table 11–3   Worker Status

Status	Meaning
Assigned	The manager assigned a task to the worker and the worker has not yet started.
Completed	The worker completed the task and the manager has not yet assigned it a new task.
Failed	The worker encountered a problem.
Fixed, Restart	You fixed the problem, and the worker will retry the task that failed.
Restarted	The worker is retrying a task or has successfully restarted a task. Note that the status does not change to Running.
Running	The worker is running a task.
Wait	The worker is idle.

If the worker shows a status of Failed, refer to Section 11.5.3, "Determining Why a Worker Failed" for assistance in fixing the problem so Oracle Fusion Applications Patch Manager can complete its processing.

11.5.3 Determining Why a Worker Failed

When a worker fails its task, you do not have to wait until the other workers and the manager stop. You can review the worker log files to determine what caused the failure. Workers do not proceed to run tasks in the subsequent phase until all tasks in the current phase complete successfully. You must take action to resolve the failure so the workers can continue to run tasks in the next phase. If the task was deferred after the worker failed, there may be no action required from you.

The first time a task fails, the manager defers the task and assigns the worker a new task. If the deferred task fails a second time, the manager defers it a second time only if the run time of the task is less than 10 minutes. If the deferred task failed a third time, or if its run time is greater than 10 minutes, the task stays at a failed status and the worker waits for manual intervention. Action by you is then required because the worker stops any further processing. An example of when this scenario can occur is during seed data upload. The seed data upload may fail due to records being locked by another process. If the lock is released before the second or third attempt of the upload, the upload succeeds.

Follow these steps to find out why a worker failed:

1. In the Log Summary, located in FA_ORACLE_ HOME/`admin/FUSION/log/logsummary_`*`fapmgr_command_`* *`timestamp`*`.html`, review the AutoPatch Apply log file to find the worker that failed. For more information, see Section 11.2.1, "Log Summary".

2. Open and review the log file for the failed worker to determine the cause of the worker failure.

   Each worker logs the status of tasks assigned to it in `adpatch_apply_` *`timestamp_workernumber`*.log. The worker log file contains information that describes exactly what task it was running and what error occurred that resulted in a failure. Review the worker log file for the failed worker to determine the source of the error. For more information, see Section 11.1.1, "Log Files for Patching Sessions".

3. Determine how to fix the problem that caused the failure.

Resolve the error using the information provided in the log files. If needed, search for the resolution at the My Oracle Support site or file a service request with Oracle Support Services if you do not understand how to resolve the issue.

4. After you resolve the problem that caused the failure, restart the failed worker.

   Select **Tell worker to restart a failed job** from the AD Controller main menu. For more information, see Section 11.5.4, "Restarting a Failed Worker".

5. Verify the worker status.

   Select **Show worker status** from the AD Controller main menu. The Status column for the worker that failed should now display Restarted or Fixed, Restart.

11.5.4 Restarting a Failed Worker

If a worker job failed or if you terminated a hanging worker process, you must manually restart the worker. Some worker processes spawn other processes called child processes. If you terminate a child process that is hung, the worker that spawned the process shows *Failed* as the status. After you fix the problem, you must restart the failed worker. After the worker restarts, the associated child processes start as well.

Follow these steps to restart a failed worker:

1. Start AD Controller. For more information, see Section 11.5.1, "Starting AD Controller".

2. Select **Show worker status** from the AD Controller main menu.

3. Take the appropriate action for each worker status:

   - If the worker status is Failed and its job has failed, select **Tell worker to restart a failed job**. When prompted, enter the number of the worker that failed.

   - If the worker status is Running or Restarted, but the job is hung, follow the steps in Section 11.5.5, "Terminating a Hung Worker Process".

11.5.5 Terminating a Hung Worker Process

When running AD utilities, there may be situations when a worker process appears to hang, or stop processing. If this occurs, you may need to terminate the process manually. After you do that, you must also restart that process manually.

> **Caution:** A process that appears to be hung could be a long-running task. Be careful when terminating processes.

To terminate a process, you start AD Controller, obtain the worker's process ID from your operating system, and then stop any hanging processes. After you make the necessary changes, you can restart the worker.

Take the following steps to terminate a worker process that is hung.

1. Start AD Controller. For more information, see Section 11.5.1, "Starting AD Controller".

2. Select **Show worker status** from the AD Controller main menu.

3. Open and review the log file for the failed worker to determine the cause of the worker failure.

   Each worker logs the status of tasks assigned to it in the `adpatch_workernumber.log`. The worker log file contains information that describes

exactly what tasks it runs and what errors occurred that resulted in a failure. Review the worker log file for the failed worker to determine the file being processed and review the worker log file to see if it is progressing. You can also verify whether the process is consuming CPU resources from your operating system.

For more information, see Section 11.1.1, "Log Files for Patching Sessions".

4. Confirm that the operating system process associated with the worker is not running. If the task is identified as "hanging", determine the worker's process ID by looking for processes being run by the worker.

```
(UNIX) ps -a| grep workernumber
(Windows) Start the Task Manager (Ctrl-Alt-Delete) to view processes.
```

5. Determine what processes the worker has started, if any. If there are child processes, get their process IDs.

6. Stop the hung process, using the command that is appropriate for your operating system.

7. If you terminate a SQL*Plus session spawned by a worker, you just need to kill the SQL*Plus session. The worker immediately detects the FAILED state. For other processes, follow Steps 7 through 11.

   In AD Controller, select **Tell manager that a worker failed its job** and enter the worker number of the hung workers. This should cause the worker to fail.

8. Select **Tell worker to quit**. When prompted, enter the worker number of the hung worker.

9. Select **Tell manager that a worker acknowledges quit**. When prompted, enter the number of the hung worker.

10. Fix the issue that caused the worker to hang. Search the My Oracle Support site or file a service request with Oracle Support Services if you do not know how to fix the issue.

11. Select **Restart a worker on the current machine**. When prompted, enter the number of the failed worker. The worker will restart its assigned tasks and spawn the associated child processes.

> **Note:** Do not select **Restart a worker on the current machine** if the worker process is running. Doing so creates duplicate worker processes with the same worker ID and will cause incorrect results.

11.5.6 Shutting Down the Manager

There may be situations when you must shut down an AD utility while it is running. For example, you may want to shut down the database while Oracle Fusion Applications is running Oracle Fusion Applications AutoPatch or during an AD Administration session. You should perform this shutdown in an orderly fashion so that it does not affect your data. The best way to do this is to shut down the workers manually.

1. Start AD Controller.

2. Select **Tell worker to quit**, and enter `all` for the worker number. The worker completes its current task and then quits.

3. Verify that no worker processes are running, using a command that is appropriate for your operating system.

4. When all the workers have shut down, the manager and the AD utility quits.

11.5.7 Reactivating the Manager

No workers are running tasks. They are either failed or waiting. A restarted worker resumes the failed task immediately if the worker process is running. Workers change to a Waiting status if they cannot run any tasks because of dependencies on a failed task, or because there are no tasks left in the phase. When no workers are able to run, the manager becomes idle.

Complete the following steps for each worker:

1. Start AD Controller. For more information, see Section 11.5.1, "Starting AD Controller".

2. Determine the cause of the error.

   Select **Show worker status**. Review the worker log file for the failed worker to determine the cause of the error.

3. Resolve the error using the information provided in the log files.

   Search for the resolution in the My Oracle Support site or file a service request with Oracle Support Services if you do not understand how to resolve the issue.

4. Restart the failed worker.

   Select **Tell worker to restart a failed job** on the AD Controller main menu. The worker process restarts, causing the AD utility and the manager to become active again.

11.5.8 Resolving the Error, "Unable to start universal connection pool"

This error occurs during patching, "Unable to start universal connection pool". Connections to the database cannot be established due to timeout limits.

Consider tuning the listener parameters `INBOUND_CONNECT_TIMEOUT_ listenername` and `SQLNET.INBOUND_CONNECT_TIMEOUT` for the server. For more information, see *Oracle Database Net Services Administrator's Guide*.

11.5.9 Resolving a Worker Blocked by a Session

When you patch database artifacts, your system should be in an idle state. If this is not the case, the patching session may hang due to locks. Examples of locks that can cause the patching session to hang are PL/SQL packages that are accessed by Oracle Enterprise Scheduler Service Server, a locked table, or a locked table row. After a specific wait time, such as 30 minutes, Oracle Fusion Applications Patch Manager performs a check to determine whether the patching session is blocked by another session. If a blocking session is found, a message describing the block is sent to the log file, as shown in the following example:

```
"[2011-03-14T02:12:18.112-07:00] [apps] [NOTIFICATION] [] [AutoPatch] Worker 4 is
blocked by session 3868 ... Please fix the session to avoid indefinite waiting
```

The worker that is blocked remains in a Running status. To resolve the issue and release the lock, stop the blocking session using the command that is appropriate for your operating system. After the blocking session is no longer running, the hung

worker proceeds to complete its task. You can use the following SQL*Plus query to identify the sessions that are blocking patching sessions:

```
SELECT blocking_session,
       sid "Blocked Session",
       module "Blocked Module",
       seconds_in_wait
 FROM gv$session
 WHERE status = 'ACTIVE'
 AND module like 'PATCHING_SESSION:%'
 AND blocking_session_status = 'VALID'
  AND user = '<FUSION schema>';
```

> **Note:** To minimize blocked sessions, ensure that you follow the steps in Step 7, "Prepare the System" before you apply a patch.

11.5.10 Resolving an Error During Conflict Checking

If you recently applied a one-off patch to a database artifact, you may encounter the following error the next time you apply a standard patch:

```
Error occurred during patch conflicts checking.
This may be due to infrastructure failure OR patch conflicts
You may check FA_ORACLE_HOME/admin/FUSION/out/patch_number_conflict_report.xml
file for any patch conflicts
You should check the file FA_ORACLE_HOME/admin/FUSION/log/adpatch.log for errors
```

A one-off database patch sets a lock on the artifact that the one-off patch updates. After you apply a one-off patch, you must subsequently apply the related standard patch that contains the same updates as the one-off to release the lock. To find out which one-off patch is locking the artifact, review the conflict_report.xml file. In the following example of this file, the one-off patch that created the lock was 909090.

```
<Patch_Conflict_Report>
  <instance>
    <appl_sys_name>FUSION</appl_sys_name>
    <appl_top>/server01/fusionapps</appl_top>
    <patch_number>909090</patch_number>
  </instance>
  <patch_type>one-off</patch_type>
  <conflict_details>
    <conflicts>
      <prod>HCM</prod>

<subdir>hcm/components/hcmPayroll/legconfig/setup/dbSchema/database/fusionDB/FUSIO
N</subdir>
      <filename>PAY_INSTALLED_LEGISLATIONS.table</filename>
      <bug>909090</bug>
    </conflicts>
```

To resolve this issue and remove the lock, obtain and apply the standard patch that delivers the same fix as the one-off patch.

11.5.11 Setting the Environment for Troubleshooting Database Issues

If you need to connect to the Oracle Fusion Applications database to troubleshoot database related issues, by running SQL*Plus, for example, you need to set up the appropriate environment variables. For setting any environment variable, run the

`adsetenv` script to generate the `APPSORA.env` file, which when sourced, sets all environment variables.

```
(UNIX)
sh adsetenv.sh
source APPSORA.env
echo $TWO_TASK

(Windows, TWO_TASK is known as LOCAL)
adsetenv.cmd
APPSORA.cmd
echo %LOCAL%
```
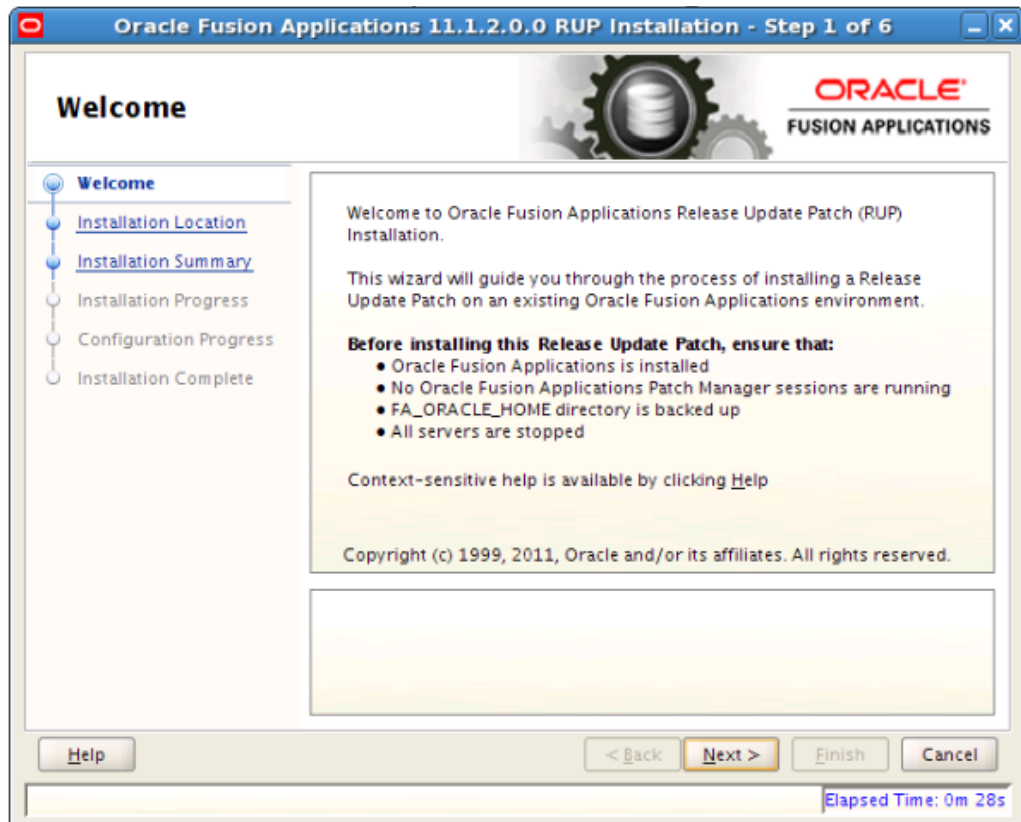
A

Release Update Patch Installer Screens

This appendix presents the Release Update Patch (RUP) Installer interview screens and describes the purpose of each of the following screens:

- Welcome

- Installation Location

- Installation Summary

- Installation Progress

- Policy Store Analysis

- Configuration Progress

- Installation Complete

A.1 Welcome

This screen appears each time you start RUP Installer the first time. This screen does not appear if you restart RUP Installer after a failure. The standard Welcome screen is read-only. It contains a navigation pane on the left-hand side that summarizes the tasks the installer will take. Each item in the pane represents an installer screen, which contains prompts for the necessary information.

Click **Next** to continue.

A.2 Installation Location

Specify the location of the existing Oracle Fusion Applications home (*FA_ORACLE_HOME*) where you want to install the RUP.

Click **Next** to continue.

A.3 Installation Summary
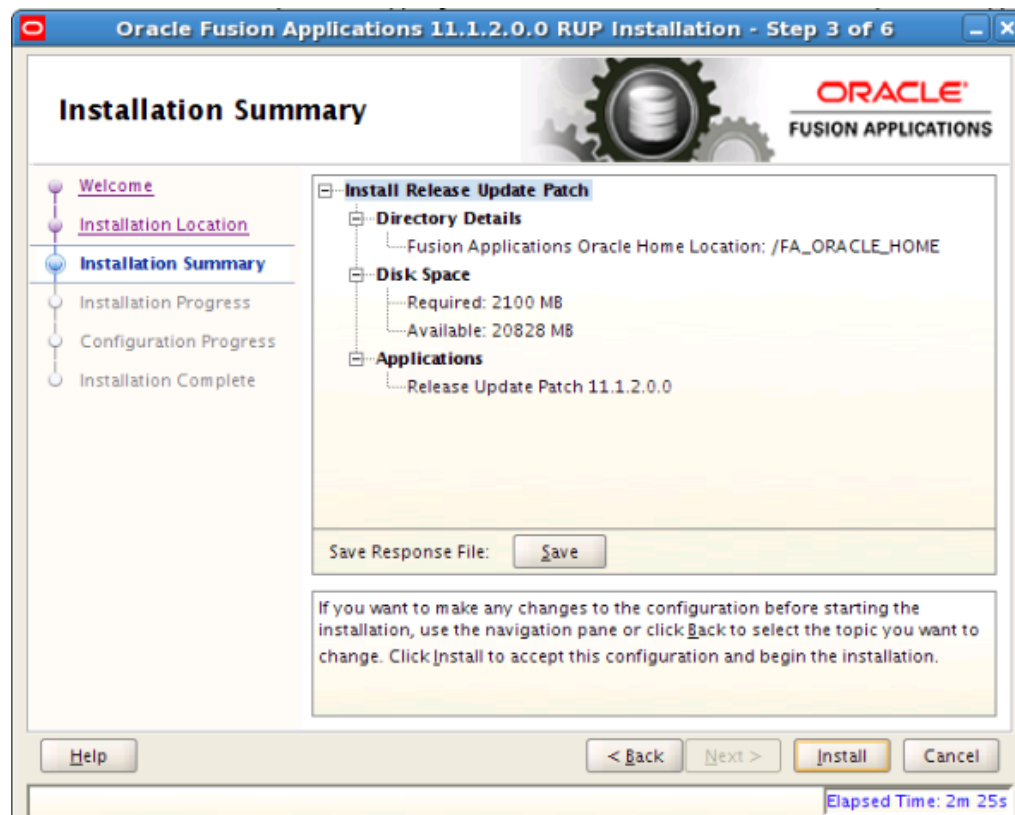
Summarizes the selections you made during this installation session. It includes the Oracle home, required and available disk space, and the version of the RUP to be installed. Review the information displayed to ensure that the installation details are what you intend.

To make changes before installing, click **Back** to return to previous screens in the interview.

Click **Install** to accept this configuration and start the installation.

A.4 Installation Progress

Displays a progress indicator that shows the percentage of the installation that is complete and indicates the location of the installation log file. The installation task consists of copying files from the RUP to the Oracle home. The configuration process starts when the installation progress indicator shows 100 percent. Click **Next** to proceed.

A.5 Policy Store Analysis

Analysis is available for the following policy store stripes: hcm, crm, fscm, and obi. Select the stripes to be analyzed and then click **Run Analysis** to identify any conflicts or deletions. Only the stripes that will be updated are enabled for analysis and the analysis could run for several minutes. After the analysis runs, review the results of the analysis to determine which deployment method RUP Installer will use for policy store changes to each stripe. Oracle recommends that you select **Apply safe changes only**. This is the safest method unless you have read and totally understood the consequences of the other three options. If you decide to resolve the conflicts or deletions before the actual JAZN upload from RUP Installer, you should run the Policy Store Analysis step again to get the most accurate analysis report. The choices for deployment method are:

- Apply safe changes only (choose this method if there are no conflicts)

- Apply all changes and overwrite customizations

- Append additive changes

- Manually resolve conflicts and upload changes using Authorization Policy Manager

If you choose **Apply safe changes only** or **Append additive changes**, then you must review the results of the analysis to manually upload any changes not applied by RUP Installer with the choice you selected, after the installation is complete. If you choose **Apply all changes and overwrite customizations**, then you may need to reapply the customizations that are overwritten after the installation is complete. If you choose one of these options, click **Next** after you make your selection.

If you choose **Manually resolve conflicts and upload changes using Authorization Policy Manager** (APM), you must pause the upgrade while you bring up the APM application and upload the changes. For more information, see the "Upgrading Oracle Fusion Applications Policies" chapter in the *Oracle Fusion Middleware Oracle Authorization Policy Manager Administrator's Guide (Oracle Fusion Applications Edition)*. Note the location of the following files:

- Baseline file: `FA_ORACLE_HOME`/admin/JAZN/`stripe`/baseline

- Patch file for fscm, crm, and hcm stripes: *FA_ORACLE_ HOME/stripe*/deploy/system-jazn-data.xml

- Patch file for the obi stripe: *FA_ORACLE_ HOME*/com/acr/security/jazn/bip_jazn-data.xml

When you complete this task in APM, shut down the APM application, return to RUP Installer, and click **Next**.

Note: If you installed a Language Pack and chose to override the base English strings in the policy store, this screen no longer displays during RUP installation.

A.6 Configuration Progress
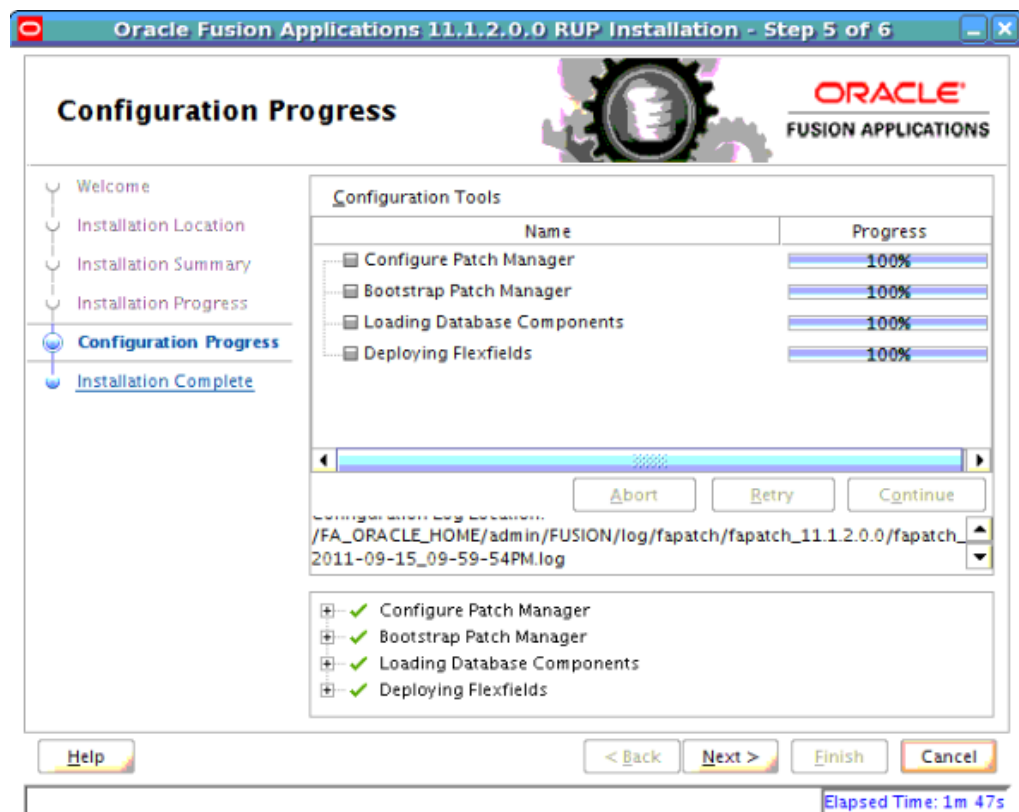
Displays a progress indicator that shows the percentage of the configuration phase that is complete. It displays each task, including steps within tasks, in the message pane as it is performed. Tasks that could be included in the configuration phase are described in Section 5.1.4, "RUP Installer Configuration Tasks" in the *Oracle Fusion Applications Patching Guide*.

Before the **Starting All Servers** task, the **Verifying Node Manager and OPMN Status** configuration task checks for access to the Node Manager and the OPMN control process. This should fail because you manually shut down these processes prior to starting RUP Installer. When this task fails, follow these steps:

1. Start the Node Manager on all hosts that are part of the Oracle Fusion Applications provisioned system. For more information, see "Start Node Manager" in *Oracle Fusion Applications Administrator's Guide*.

2. Restart the OPMN server for BI and GOP, and the OPMN server plus managed processes for webtier. This is similar to the `stop` steps described in Section 5.3.3.2, "Stop the Node Manager and the OPMN Control Process" in the *Oracle Fusion Applications Patching Guide*, except that for BI and GOP, you must start only the OPMN server itself, while for webtier, you should start OPMN and all processes that it manages. If you run the webtier (OHS) installed with the Oracle Fusion Applications middle tier, you can start it using the following steps. If you run the webtier on a separate machine, you may be able to run the steps below on the other machine. In either case, ensure that webtier (OHS) is up at this point.

Example for BI: (note the usage of `start` instead of `startall`)

```
cd APPLICATIONS_BASE/instance/BIInstance/bin
./opmnctl start
```

Example for GOP: (note the usage of `start` instead of `startall`)

```
cd APPLICATIONS_BASE/instance/gop_1/bin
./opmnctl start
```

Example for webtier:

```
cd APPLICATIONS_BASE/instance/CommonDomain_webtier/bin
./opmnctl startall
```

For more information about the location of `APPLICATIONS_BASE`, see Section 2.1.2, "Oracle Fusion Applications Oracle Home" in the *Oracle Fusion Applications Patching Guide*.

The BI processes managed by OPMN are started by RUP installer in the Start All Servers configuration task. The GOP processes managed by OPMN can be started by an administrative user from the GOP home page in Oracle Enterprise Manager after RUP installer completes.

3. Fix any other environment issues before retrying the session. If RUP Installer exits for any reason, make sure that all node managers and OPMN processes are running. Contact Oracle Support Services to proceed out of this step if you have environment issues.

4. After you start these services, click **Retry** to move to the **Starting All Servers** task.

No additional user action is required in the Configuration Progress screen unless a failure occurs. For more information, see Section 5.5.3, "General Troubleshooting During the Configuration Phase" in the *Oracle Fusion Applications Patching Guide*.

A.7 Installation Complete
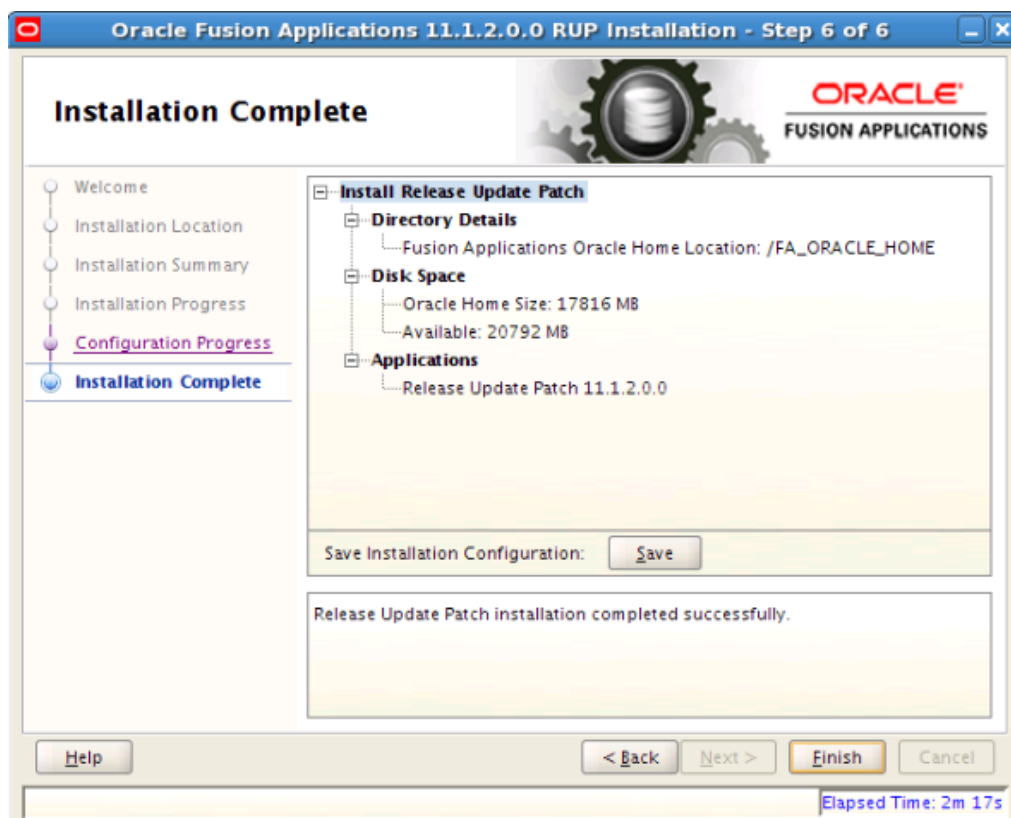
Summarizes the installation just completed. If you want to save this configuration to a response file, click **Save**. For more information, see "How Response Files Work" in the *Oracle Database Installation Guide 11g Release 2 (11.2) for Linux*.

To complete a successful installation, click **Finish**. The **Finish** button is activated only if all mandatory configuration tasks completed successfully. If you want to rerun this session to resolve failed configuration tasks, click **Cancel.**

B

Language Pack Installer Screens

This appendix presents the Language Pack Installer screens and describes the purpose of each of the following screens:

- Welcome

- Installation Location

- Installation Summary

- Installation Progress

- Policy Store Analysis

- Configuration Progress

- Installation Complete

B.1 Welcome

This screen appears each time you start Language Pack Installer the first time. This screen does not appear if you restart Language Pack Installer after a failure. The standard Welcome screen is read-only. It contains a navigation pane on the left-hand

side that summarizes the tasks the installer will take. Each item in the pane represents an installer screen, which contains prompts for the necessary information.
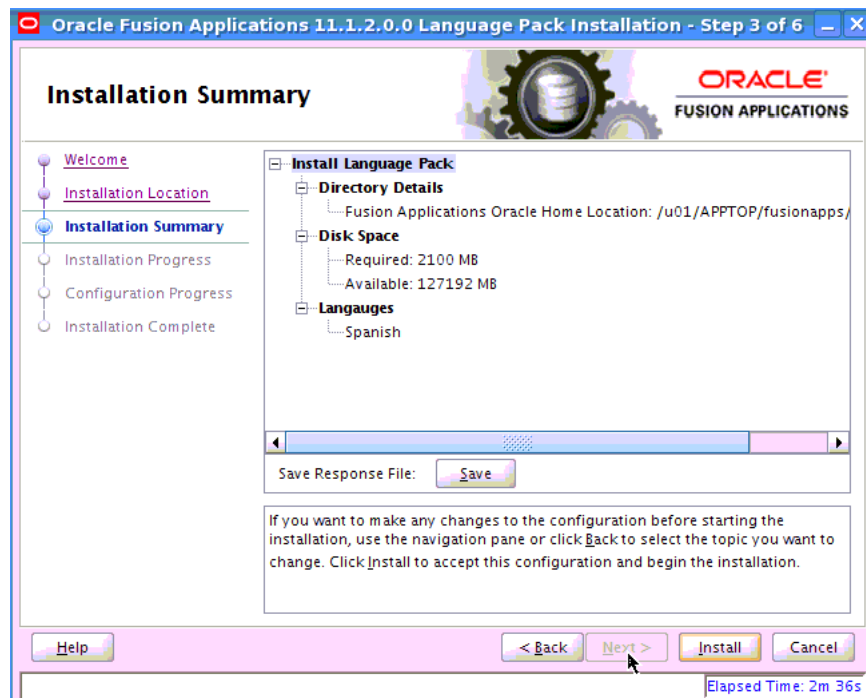
Click **Next** to continue.

B.2 Installation Location

Specify the location of the existing Oracle Fusion Applications home (*FA_ORACLE_ HOME*) where you want to install the language.

Click **Next** to continue.

B.3 Installation Summary

Summarizes the selections you made during this installation session. It includes the Oracle home, required and available disk space, and the language to be installed. Review the information displayed to ensure that the installation details are what you intend.

To make changes before installing, click **Back** to return to previous screens in the interview.
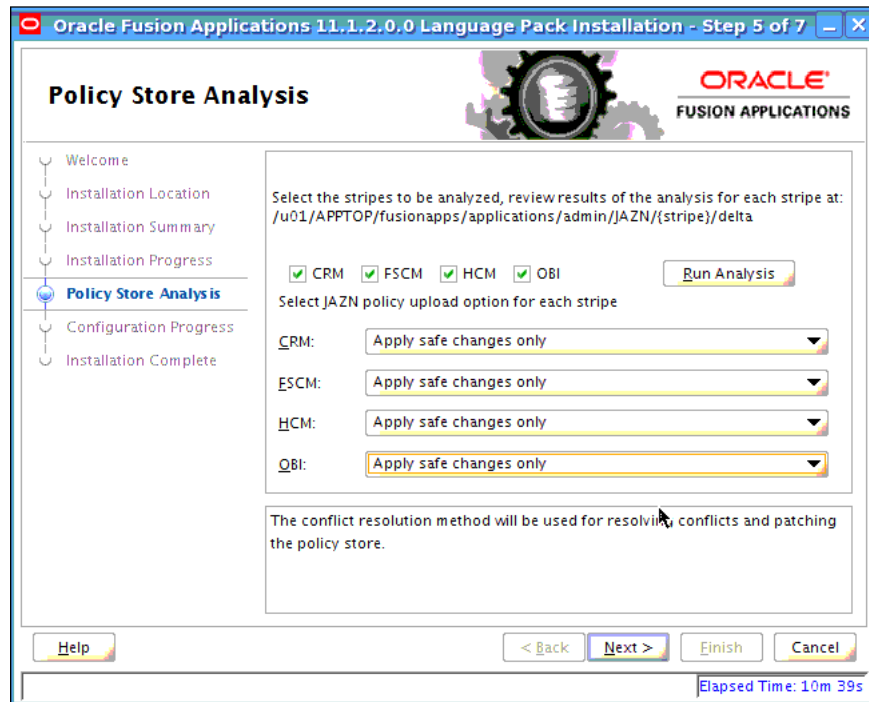
Click **Install** to start installing this language.

B.4 Installation Progress

Displays a progress indicator that shows the percentage of the installation that is complete and indicates the location of the installation log file. The installation task consists of copying files from the Language Pack to the Oracle home. The configuration process starts when the installation progress indicator shows 100 percent. Click **Next** to continue.

B.5 Policy Store Analysis

Note that this screen displays only when the `J-DupdateJAZNPolicyStore` option is set to `true` with the `runinstaller` command.

Analysis is enabled for the following stripes: hcm, crm, fscm, and obi. Select the stripes to be analyzed and then click **Run Analysis** to identify any conflicts or deletions. Only the stripes that are included in the language pack are enabled for analysis and the analysis could run for several minutes. After the analysis runs, review the results of the analysis and decide which deployment method you want Language Pack Installer to use for policy store changes to each stripe. Oracle recommends that you select **Apply safe changes only**. This is the safest method unless you have read and totally understood the consequences of the other three options. If you decide to resolve the conflicts or deletions before the actual JAZN upload from Language Pack installer, you should run the Policy Store Analysis step again to get the most accurate analysis report. The choices for deployment method are:

- Apply safe changes only (choose this method if there are no conflicts)
- Apply all changes and overwrite customizations
- Append additive changes
- Manually resolve conflicts and upload changes using Authorization Policy Manager.

If you choose **Apply safe changes only** or **Append additive changes**, then you must review the results of the analysis to manually upload any changes not applied by Language Pack Installer with the choice you selected, after the installation is complete. If you choose **Apply all changes and overwrite customizations**, then you may need to reapply the customizations that are overwritten after the installation is complete. If you choose one of these options, click **Next** after you make your selection.
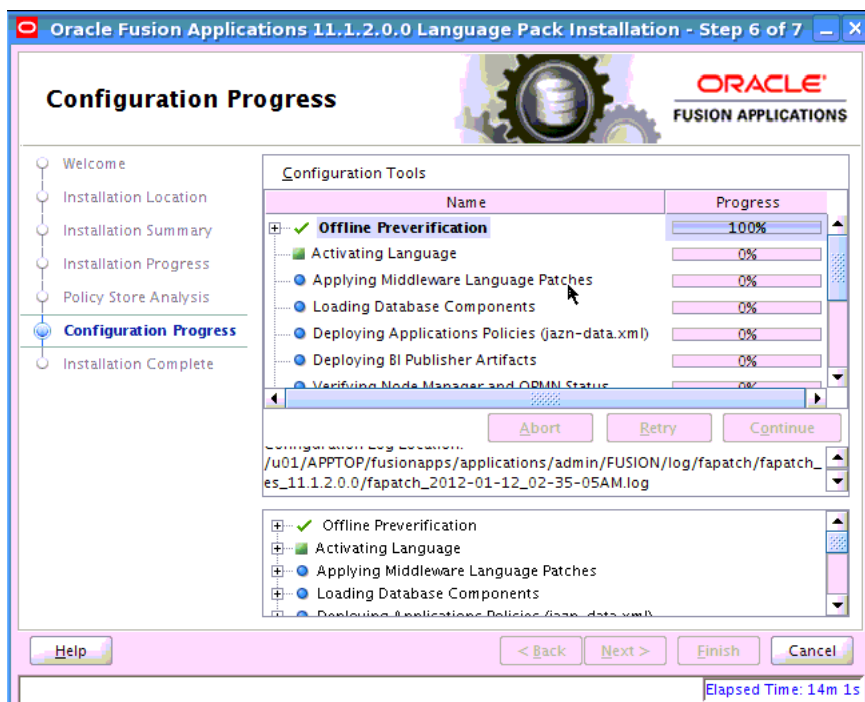
If you choose **Manually resolve conflicts and upload changes using Authorization Policy Manager** (APM), you must pause the installation while you bring up the APM application and upload the changes. For more information, see the "Upgrading Oracle

Fusion Applications Policies" chapter in the *Oracle Fusion Middleware Oracle Authorization Policy Manager Administrator's Guide (Oracle Fusion Applications Edition)*. Note the location of the following files:

- Baseline file: `FA_ORACLE_HOME`/admin/JAZN/`stripe`/baseline

- Patch file for fscm, crm, and hcm stripes: `FA_ORACLE_HOME`/`stripe`/deploy/system-jazn-data.xml

- Patch file for the obi stripe: `FA_ORACLE_HOME`/com/acr/security/jazn/bip_jazn-data.xml

When you complete this task in APM, shut down the APM application, return to Language Pack Installer, and click **Next**.

B.6 Configuration Progress

Displays a progress indicator that shows the percentage of the configuration that is complete. It displays each task in the message pane as it is performed. Tasks that could be included in the configuration phase are described in Section 6.1.5, "Language Pack Installer Configuration Tasks in the *Oracle Fusion Applications Patching Guide*.

Before the **Starting All Servers** task, the **Verifying Node Manager and OPMN Status** configuration task checks for access to the Node Manager and the OPMN control process. This should fail because you manually shut down these processes prior to starting Language Pack Installer. Do not cancel and exit out of Language Pack Installer in response to this task.

When this task fails, follow these steps:

1. Start the Node Manager on all hosts that are part of the Oracle Fusion Applications provisioned system. For more information, see "Start Node Manager" in *Oracle Fusion Applications Administrator's Guide*.

2. Restart the OPMN server for BI and GOP, and the OPMN server plus managed processes for webtier. This is similar to the `stop` steps described in Step 2, Section

5.3.1, "Before You Begin", except that for BI and GOP, you must start only the OPMN server itself, while for webtier, you should start OPMN and all processes that it manages. If you run the webtier (OHS) installed with the Oracle Fusion Applications middle tier, you can start it using the following steps. If you run the webtier on a separate machine, you may be able to run the steps below on the other machine. In either case, ensure that webtier (OHS) is up at this point.

Example for BI: (note the usage of `start` instead of `startall`)

```
cd APPLICATIONS_BASE/instance/BIInstance/bin
./opmnctl start
```

Example for GOP: (note the usage of `start` instead of `startall`)

```
cd APPLICATIONS_BASE/instance/gop_1/bin
./opmnctl start
```

Example for webtier:

```
cd APPLICATIONS_BASE/instance/CommonDomain_webtier/bin
./opmnctl startall
```

For more information about the location of *APPLICATIONS_BASE*, see Section 2.1.2, "Oracle Fusion Applications Oracle Home" in the *Oracle Fusion Applications Patching Guide*.

The BI processes managed by OPMN are started by Language Pack Installer in the Start All Servers configuration task. The GOP processes managed by OPMN can be started by an administrative user from the GOP home page in Oracle Enterprise Manager after Language Pack Installer completes.

3. Fix any other environment issues before retrying the session. If Language Pack Installer exits for any reason, make sure that all node managers and OPMN processes are running. Contact Oracle Support Services to proceed out of this step if you have environment issues.

4. After you start these services, click **Retry** to move to the **Starting All Servers** task. If starting of servers times out, see Section 5.4.10, "Failure During Starting All Servers" in the *Oracle Fusion Applications Patching Guide*.

No additional user action is required in the Configuration Progress screen unless a failure occurs. For more information, see Section 5.4.3, "Failure During the Configuration Phase" in the *Oracle Fusion Applications Patching Guide*.

B.7 Installation Complete
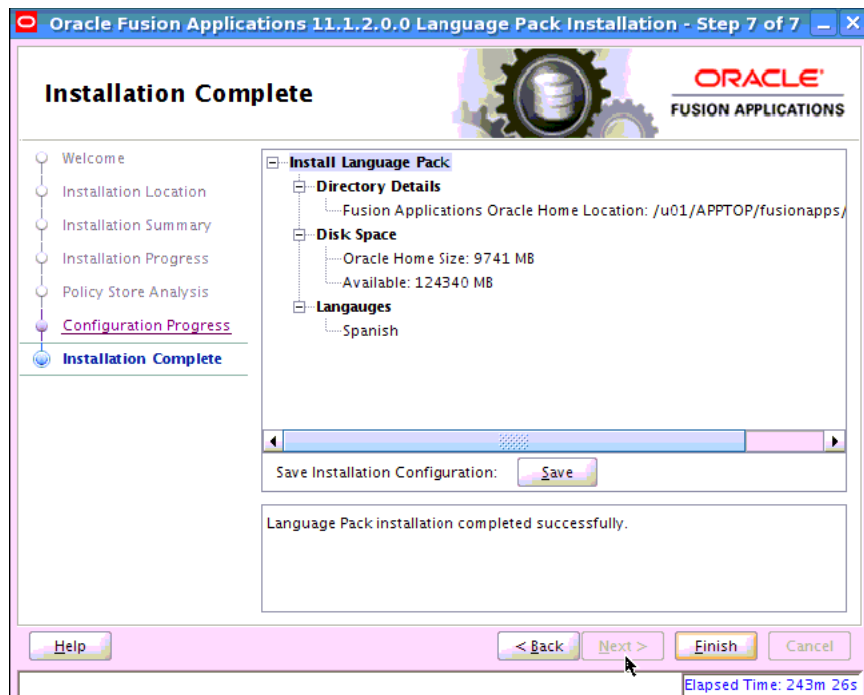
Summarizes the installation just completed. If you want to save this configuration to a response file, click **Save**. For more information, see "How Response Files Work" in the *Oracle Database Installation Guide 11g Release 2 (11.2) for Linux*.

To complete a successful installation, click **Finish**. If you want to rerun this session after you resolve failed configuration tasks, click **Cancel.**