Oracle® Fusion Middleware

Installation Guide for Oracle Enterprise Content Management Suite

11*g* Release 1 (11.1.1)

E14495-02

February 2010

ORACLE®

Oracle Fusion Middleware Installation Guide for Oracle Enterprise Content Management Suite 11*g* Release 1 (11.1.1)

E14495-02

Primary Author: Bonnie Vaughan

Contributing Authors: Deanna Burke, Sarah Howland, Kevin Hwang, Janet Maltz, Bruce Silver, Martin Wykes

Contributors: Tom Albrecht, , Satheesh Amilineni, Alex Barnett, Pete Chapman, Sandra Christiansen, Eric Cloney, Rupesh Das, Carl Foster, Sudhanshu Garg, Brian Gray, Helen Grembowicz, Marsha Hancock, Mary Hoepner, Mei Hong, David Jones, Vasant Kumar, Peter LaQuerre, Bill Loi, Rene Madsen, Liju Nair, Saskia Nehls, Bob O'Kane-Trombley, Toby O'Sullivan, Jason Ogaard, Alejandro Paredes, Andy Peet, Sancho Pinto, Wes Prichard, Rafael Ramirez, Indira Smith, Gene Sutay, Matt Wall, Venkatesh Yadalam

Contents

4   Configuring Oracle Enterprise Content Management Suite

5   Configuring Oracle Imaging and Process Management

6   Configuring Oracle Information Rights Management

7   Verifying the Installation and Configuration

8   Deinstalling Oracle Enterprise Content Management Suite

9   Migrating a Domain from Test to Production

A   Oracle Enterprise Content Management Suite Installation Screens

Preface

The *Oracle Fusion Middleware Installation Guide for Oracle Enterprise Content Management Suite* provides information and instructions for installing, configuring, and troubleshooting Oracle Enterprise Content Management Suite.

Audience

This guide is intended for users who are installing Oracle Enterprise Content Management Suite for the first time and are comfortable running some system administration operations, such as creating users and groups, adding users to groups, and installing operating system patches on the computer where your products will be installed. Users who are installing on a UNIX operating system need `root` access to run some scripts.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at http://www.oracle.com/accessibility/.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request

process. Information about TRS is available at
http://www.fcc.gov/cgb/consumerfacts/trs.html, and a list of phone
numbers is available at http://www.fcc.gov/cgb/dro/trsphonebk.html.

Related Documents

For additional information, see the following documents:

- *Oracle Fusion Middleware Administrator's Guide*

- *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*

- *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter*

- *Oracle Fusion Middleware Concepts*

- *Oracle Fusion Middleware E-Business Suite Adapter for Oracle Enterprise Content Management Administrator's Guide*

- *Oracle Fusion Middleware High Availability Guide*

- *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*

- *Oracle Fusion Middleware Installation Planning Guide*

- *Oracle Fusion Middleware Node Manager Administrator's Guide for Oracle WebLogic Server*

- *Oracle Fusion Middleware Quick Installation Guide for Oracle Enterprise Content Management Suite*

- *Oracle Fusion Middleware Repository Creation Utility User's Guide*

- *Oracle Fusion Middleware Securing Oracle WebLogic Server*

- *Oracle Fusion Middleware Security Guide*

- *Oracle Fusion Middleware Using Clusters for Oracle WebLogic Server*

- *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*

Conventions

In this document, the term **UNIX system** or **UNIX operating system** refers to a
category of operating systems that includes Linux operating systems.

The following table describes the text conventions that this document uses.

Convention	Meaning
boldface	Boldface type indicates a graphical user interface element associated with an action or a term defined in the text or glossary.
italic	Italic type indicates a book title, emphasis, or a placeholder variable for which you can supply a value.
monospace	Monospace type indicates a command within a paragraph, a URL, code in an example, text that appears on the screen, or text that you enter.

1

Installation Overview

Oracle Enterprise Content Management Suite, an Oracle Fusion Middleware component, is an integrated suite of products designed for managing content. This chapter provides an overview of the procedures for installing Oracle Enterprise Content Management Suite and configuring its products as applications deployed to Oracle WebLogic Server domains.

This chapter includes the following sections:

- Section 1.1, "Oracle Enterprise Content Management Suite Applications"
- Section 1.2, "Installation Roadmap"
- Section 1.3, "Installation Modules"
- Section 1.4, "Oracle WebLogic Server Domain"
- Section 1.5, "Directory Structure for Oracle Enterprise Content Management Suite"

1.1 Oracle Enterprise Content Management Suite Applications

Oracle Enterprise Content Management Suite includes the following products:

- Oracle Imaging and Process Management (Oracle I/PM)

  Oracle I/PM is an integrated framework of client software modules with a customizable user interface for managing documents from image capture to archiving. Client modules can be integrated within this framework to provide a single user interface, including third-party information systems, imaging, workflow process, and enterprise content management.

- Oracle Information Rights Management (Oracle IRM)

  Oracle IRM secures and tracks sensitive digital information everywhere it is stored and used. The installation of Oracle IRM Desktop agent software is required on every end user device on which sealed information is created or used.

After you install these products on your system, you can configure one or more of them as applications deployed to a previously installed Oracle WebLogic Server.

1.2 Installation Roadmap

Table 1–1 describes the high-level tasks for installing and configuring Oracle Enterprise Content Management Suite. You need to perform the tasks in order except as noted. The table also provides information on where to get more details on each task.

Table 1–1   Oracle Enterprise Content Management Suite Installation Procedure

Task	Description	Mandatory/ Optional?	Documentation
Task 1 - Prepare your system environment for installation	Ensure that your system environment meets the general installation requirements for Oracle Fusion Middleware, for Oracle Enterprise Content Management Suite, and for Repository Creation Utility (RCU), which requires a supported database.	Mandatory	Section 3.1, "Preparing for Installation."
Task 2 - Create schemas for applications	Oracle Enterprise Content Management Suite applications require schemas that must be installed in a supported database, such as Oracle Database or Microsoft SQL Server. Prepare a database for Oracle Enterprise Content Management Suite schemas, then install RCU and use it to create schemas. **Note:** You can perform this task before or after Task 3 - Install Oracle WebLogic Server in a Middleware home and Task 4 - Install Oracle Enterprise Content Management Suite.	Mandatory	Section 1.3.2, "Database" Chapter 2, "Creating Schemas for Oracle Enterprise Content Management Suite"
Task 3 - Install Oracle WebLogic Server in a Middleware home	Oracle Enterprise Content Management Suite runs on Oracle WebLogic Server. You must install Oracle WebLogic Server before you install Oracle Enterprise Content Management Suite. The installer creates the Oracle WebLogic Server home directory (*WL_HOME*) within the Middleware home directory (*MW_HOME*). **Note:** You can perform this task before or after Task 2 - Create schemas for applications.	Mandatory	Section 3.1.2, "Installing Oracle WebLogic Server in a Middleware Home"
Task 4 - Install Oracle Enterprise Content Management Suite	Use the Oracle Fusion Middleware 11g Oracle Enterprise Content Management Suite Installer to install Oracle Enterprise Content Management Suite. Within the Middleware home, the installer creates an Oracle home directory named `Oracle_ECM`, where it installs the Oracle Enterprise Content Management Suite products. The installer lays down the Oracle Enterprise Content Management Suite binaries for these products: ■ Oracle I/PM ■ Oracle IRM **Note:** You can perform this task before or after Task 2 - Create schemas for applications, but you need to perform it after Task 3 - Install Oracle WebLogic Server in a Middleware home.	Mandatory	Chapter 3, "Installing Oracle Enterprise Content Management Suite"

Table 1–1 (Cont.) Oracle Enterprise Content Management Suite Installation Procedure

Task	Description	Mandatory/ Optional?	Documentation
Task 5 - Configure Oracle Enterprise Content Management Suite	Create or extend an Oracle WebLogic Server domain and choose the products that you want to deploy and configure as applications. Fusion Middleware Configuration Wizard creates an Oracle WebLogic Server domain, which contains the Administration Server and one or more Managed Servers, such `IRM_server1`, depending on the products that you choose. After you have created a domain, you can later extend that domain to deploy and configure additional Oracle Enterprise Content Management Suite products as applications.	Mandatory	Chapter 4, "Configuring Oracle Enterprise Content Management Suite"
Task 6 - Install and configure an external LDAP-based identity store	By default, Oracle Enterprise Content Management Suite uses the Oracle WebLogic Server embedded LDAP server. Although secure, the out-of-the-box embedded LDAP may not scale appropriately for enterprise production environments. To manage the identities of users across diverse servers and enable single sign-on across applications, you can install and configure an external LDAP-based identity store. **Note:** If you perform this task before Task 7 - Perform Postinstallation Configuration and Task 8 - Verify the installation, the postinstallation configuration is easier.	Optional	Section 4.4, "Reassociating the Identity Store with an External LDAP Authentication Provider."
Task 7 - Perform Postinstallation Configuration	For each Oracle Enterprise Content Management Suite application, you need to perform some initial configuration to get the application up and running in the Managed Server. Some of this initial configuration needs to be done before you start the Managed Server for the first time.	Mandatory	Chapter 5, "Configuring Oracle Imaging and Process Management" Chapter 6, "Configuring Oracle Information Rights Management"
Task 8 - Verify the installation	To verify the installation, you can start the Administration Server and Managed Servers. Before you can start a Managed Server the first time, you must start the Administration Server. To start working with an Oracle Enterprise Content Management Suite application, you must start the Managed Server to which that application is deployed. You can then access the application's URL and complete the configuration according to your requirements.	Mandatory	Chapter 7, "Verifying the Installation and Configuration"

1.3 Installation Modules

The following installation modules are required for installing the products in Oracle Enterprise Content Management Suite:

- Oracle Fusion Middleware and Oracle WebLogic Server Homes

- Database

- Repository Creation Utility

- Oracle Enterprise Content Management Suite

- Oracle Universal Content Management 10g for Oracle I/PM Repository

1.3.1 Oracle Fusion Middleware and Oracle WebLogic Server Homes

Oracle Enterprise Content Management Suite requires a Middleware home with Oracle WebLogic Server on your system. If your system does not already have Oracle WebLogic Server, you can install it in a new Middleware home directory, as described in Section 3.1.2, "Installing Oracle WebLogic Server in a Middleware Home."

A Middleware home is a container for the Oracle WebLogic Server home, and, optionally, one Oracle Common home and one or more Oracle homes, with a directory structure like this:

```
/middleware_home
    wlserver_10.3
    jdk160
    oracle_common
    ECM_ORACLE_HOME
    user_projects
```

The ECM Oracle home contains the binary and library files necessary for Oracle Enterprise Content Management Suite. *ECM_ORACLE_HOME* represents the ECM Oracle home in path names.

The ECM Oracle home can be associated with multiple Oracle WebLogic

Server domains. The Oracle Common home contains the binary and library files required for Oracle Enterprise Manager 11*g* Fusion Middleware Control and Java Required Files (JRF).

A Middleware home can reside on a local file system or on a remote shared disk that is accessible through a network file system (NFS).

For more information about the structure and contents of a Middleware home, see "Understanding Oracle Fusion Middleware Concepts" in *Oracle Fusion Middleware Administrator's Guide*.

1.3.2 Database

The configuration of Oracle Enterprise Content Management Suite requires the availability of a supported database. The database must be up, and a database instance must be running. It does not have to be on the same machine where you are installing the suite.

The database must also be compatible with Repository Creation Utility (RCU), which creates the schemas for the suite's applications. For more information, see Chapter 2, "Creating Schemas for Oracle Enterprise Content Management Suite."

> **Note:** RCU is available only on a Linux or Windows operating system. You can use either the Linux-based RCU or Windows-based RCU to create schemas in any supported database.

For the latest information about supported databases, see the Oracle Fusion Middleware Supported System Configurations page on Oracle Technology Network at

http://www.oracle.com/technology/software/products/ias/files/fusion_certification.html

For more information about Oracle Database, see the Oracle Database Documentation page on Oracle Technology Network at

http://www.oracle.com/technology/documentation/database.html

1.3.3 Repository Creation Utility

You need to install and run Repository Creation Utility (RCU) to create a database schema for each Oracle Enterprise Content Management Suite application that you plan to configure.

RCU is available only on a Linux or Windows operating system. You can use RCU from a Linux or Windows system to create schemas in a supported database installed on any operating system.

For information about installing and running RCU, see Chapter 2, "Creating Schemas for Oracle Enterprise Content Management Suite."

1.3.4 Oracle Enterprise Content Management Suite

Installation of Oracle Enterprise Content Management Suite copies the files for all of the products in the suite to your system. To use one or more these products, you need to configure each one to run in a Managed Server, as an application deployed to Oracle WebLogic Server.

1.3.5 Oracle Universal Content Management 10g for Oracle I/PM Repository

Oracle I/PM uses Oracle Universal Content Management (Oracle UCM) for its repository. Therefore, your system needs to have Oracle UCM configured before the configuration of Oracle I/PM.

The Oracle Fusion Middleware 11*g* media packs include the Oracle UCM 10*g* media parts listed in Table 1–2.

Table 1–2   Oracle UCM 10g Media Parts in Oracle Fusion Middleware 11g

Part number	Media Part
V13682-01	Oracle Content Server 10gR3 (10.1.3.3.3) for Microsoft Windows (32-bit)
V13684-01	Oracle Content Server 10gR3 (10.1.3.3.3) for Linux x86 (32-bit) and Linux x86-64
V13687-01	Oracle Content Server 10gR3 (10.1.3.3.3) for IBM zSeries Based Linux
V13683-01	Oracle Content Server 10gR3 (10.1.3.3.3) for Solaris Operating Environment (SPARC 64-bit)

Table 1–2   (Cont.) Oracle UCM 10g Media Parts in Oracle Fusion Middleware 11g

Part number	Media Part
V13688-01	Oracle Content Server 10gR3 (10.1.3.3.3) for Solaris Operating Environment (x86)
V13685-01	Oracle Content Server 10gR3 (10.1.3.3.3) for AIX5L Based Systems (64-bit)
V13686-01	Oracle Content Server 10gR3 (10.1.3.3.3) for HP-UX PA-RISC (64-bit)
V13689-01	Oracle Content Server 10gR3 (10.1.3.3.3) for HP-UX Itanium (64-bit)

All other Oracle UCM 10*g* components that Oracle I/PM 11*g* requires are on separate media parts. The ContentServerUpdateBundle component includes Content Tracker and all Oracle Content Server fixes since Release 10.1.3.5.0.

For information about installing Oracle UCM 10*g*, see the Oracle Universal Content Management page on Oracle Technology Network at

http://www.oracle.com/technology/products/content-management/ucm/index.html

1.4 Oracle WebLogic Server Domain

Each Oracle WebLogic Server domain includes an Administration Server and one or more Managed Servers. You can configure each Oracle Enterprise Content Management Suite application on a Managed Server by creating or extending a domain.

After you create a domain, you can use the Oracle WebLogic Server Administration Console and Oracle Fusion Middleware 11g Fusion Middleware control to perform postinstallation tasks on the domain. You can also use WebLogic Scripting Tool commands to perform some of the postinstallation tasks.

1.5 Directory Structure for Oracle Enterprise Content Management Suite

Figure 1–1 shows the directory structure of an Oracle Enterprise Content Management Suite installation.

When you install Oracle WebLogic Server, the installer creates a Middleware home directory (*MW_HOME*) that contains the Oracle WebLogic Server home directory (*WL_HOME*) and an Oracle Common home directory (*ORACLE_COMMON_HOME*), which contains the binary and library files required for the Oracle Enterprise Manager Fusion Middleware Control and Java Required Files (JRF).

When you install Oracle Enterprise Content Management Suite, an ECM Oracle home directory for the suite (*ECM_ORACLE HOME*) is created under the Middleware home directory. The ECM Oracle home directory contains the binary and library files for Oracle Enterprise Content Management Suite.

When you configure Oracle Enterprise Content Management Suite to create an Oracle WebLogic Server domain, a domain directory is created under the *MW_HOME*/user_ projects/domain directory. The directory for the domain where you configure Oracle Enterprise Content Management Suite contains the Administration Server and one or more Managed Servers, each hosting an Oracle Enterprise Content Management Suite application. Based on the application or applications that you install, the following Managed Servers are created:

- Oracle I/PM Managed Server
- Oracle IRM Managed Server

Figure 1–1 illustrates the directory structure that installation and configuration of these products will create on your system. Numbers in the figure show the order in which to perform certain tasks.

Figure 1–1   Directory Structure of an Oracle Enterprise Content Management Suite Installation
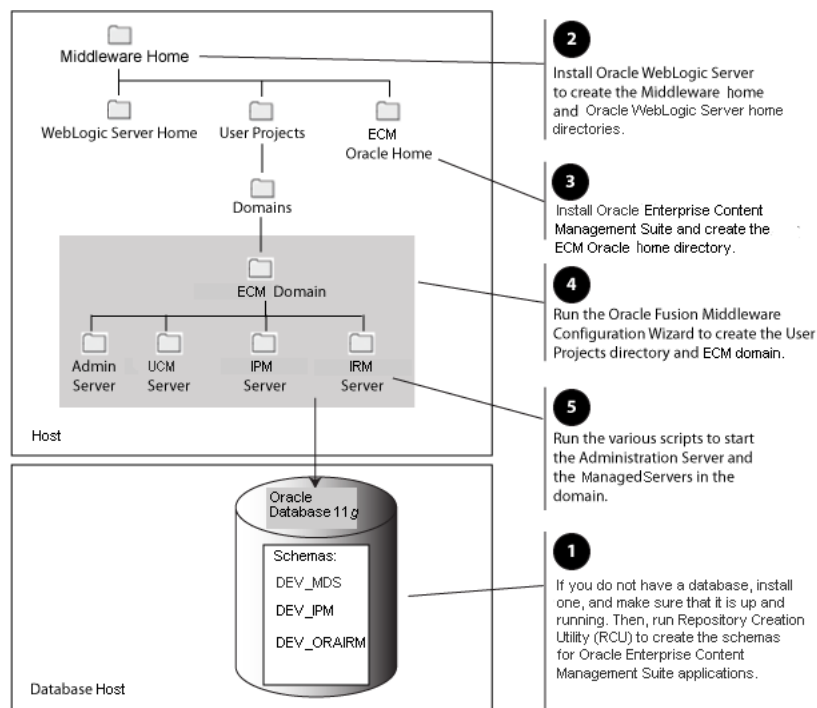
The topology in Figure 1–1 includes multiple applications configured on the same host in one Oracle WebLogic Server domain that includes only Oracle Enterprise Content Management Suite applications. The schemas for the applications are in the same database.

2

Creating Schemas for Oracle Enterprise Content Management Suite

This chapter explains how to use Repository Creation Utility (RCU) to create database schemas for Oracle Enterprise Content Management Suite applications.

This chapter includes the following sections:

- Section 2.1, "Preparing to Run Repository Creation Utility and Load Schemas"
- Section 2.2, "Creating Oracle Enterprise Content Management Suite Schemas"

2.1 Preparing to Run Repository Creation Utility and Load Schemas

Oracle Enterprise Content Management Suite requires that an application schema exists in the database prior to configuration of the application. You must run RCU to create a schema in the database.

Before running RCU and loading any application schemas, make sure your system meets the prerequisites for RCU and the application or applications.

2.1.1 Database Prerequisites

Installation of Oracle Enterprise Content Management Suite requires the availability of a supported database. This database must be up and running, and it does not have to be on the same system where you are installing the products. The database must also be compatible with RCU, which you need to use to create the schemas necessary for Oracle Enterprise Content Management Suite products.

For information about supported databases, see the "System Requirements and Supported Platform" document for your product on the Oracle Fusion Middleware Supported System Configurations page on Oracle Technology Network at

http://www.oracle.com/technology/software/products/ias/files/fusion_
certification.html

2.1.2 RCU for Linux and Windows Operating Systems

RCU is available only on a Linux or Windows operating systems. You can use RCU from a Linux or Windows system to create schemas in a supported database installed on any operating system.

2.2 Creating Oracle Enterprise Content Management Suite Schemas

Oracle Enterprise Content Management Suite requires that an application schema exists in the database before configuration of the application. You must run Repository Creation Utility (RCU) to create application schemas in the database. The following procedure describes to create schemas in Oracle Database.

To create Oracle Enterprise Content Management Suite schemas:

1. Insert the Repository Creation Utility DVD, and then start RCU from the `bin` or `BIN` directory in the `rcuHome` directory.

    To start RCU on a UNIX operating system:

    ```
    cd rcuHome/bin
    ./rcu
    ```

    To start RCU on a Windows operating system:

    ```
    cd rcuHome\BIN
    rcu.bat
    ```

    You can also download a ZIP file containing Repository Creation Utility from the Oracle Fusion Middleware 11*g* Software Downloads page on Oracle Technology Network at

    http://www.oracle.com/technology/software/products/middleware

    > **Note:** On a Windows operating system, do not unzip the RCU ZIP file to a directory with a name that contains spaces.

    After downloading the ZIP file, extract the contents to a directory of your choice, and then run RCU as the preceding text describes.

2. Welcome screen

    Click **Next**.

3. Create Repository screen

    Select **Create**.

    Click **Next**.

4. Database Connection Details screen

    Database Type: Specify a supported database. The default is `Oracle Database`. For information about supported databases, see Section 2.1.1, "Database Prerequisites."

    For connecting to a database instance, provide the following information:

    - **Host Name:** Specify the name of the machine on which your database resides, in the format `host.example.com`. F

      For Oracle Real Application Cluster (RAC) databases, specify the Virtual IP name or one of the node names.

    - **Port:** Specify the database listen port number. The default port number for an Oracle Database instance is `1521`. The default port number for a Microsoft SQL Server instance is `1433`.

- **Service Name:** For Oracle Database, specify the service name, which is typically the same as the global database name. For Microsoft SQL Server, specify a database name because there is no service name.

  If you do not know the service name for your Oracle Database, you can obtain it from the SERVICE_NAMES parameter in the database's initialization parameter file. If this file does not contain the SERVICE_NAMES parameter, then the service name is the same as the global database name, which is specified in the DB_NAME and DB_DOMAIN parameters.

  For Oracle RAC databases, specify the service name of one of the nodes in this field; for example, sales.example.com.

- **Username:** Specify the user name of the database administrator.

  For Oracle Database, specify the name of a user with DBA or SYSDBA privileges. The default user name with SYSDBA privileges is SYS.

- **Password:** Specify the password for your database user.

- **Role:** Select a database user role from the list.

  SYS requires the SYSDBA role.

Click **Next**. The Checking Global Prerequisites dialog box appears.

If you have any prerequisite errors, the Database Connection Details screen displays details about the errors. Fix any errors, then click **Next** again.

After the checking is complete with no errors, click **OK** to dismiss the dialog box and go to the next screen.

5. Select Components screen

   Near the top of the screen, select **Create a New Prefix**, and specify a prefix, or leave the default prefix, DEV.

   The prefix can contain from 1 to 12 alphanumeric characters (0-9, a-z, or A-Z). No white space or special characters are allowed. RCU displays your prefix later with an underline character appended. For example, RCU would display the default prefix as DEV_.

   Expand **Enterprise Content Management** in the Components list, and select one or more applications for which to create a schema:

   - **Oracle Information Rights Management**

   - **Oracle Imaging and Process Management**

   Also, for Oracle WSM Policy Manager, expand **AS Common Schemas**, and select **Metadata Services**.

   Your database must contain a schema for an application before you configure it.

   > **Note:** Record each schema name from this screen because you will need it later, in the format *schemaprefix_schemasuffix*, to configure the corresponding application. For example, if you used the default prefix, DEV_, you would supply the following name for the Oracle IRM schema:
   >
   > DEV_ORAIRM

   Click **Next**. The Checking Component Prerequisites dialog box appears.

If you have any prerequisite errors, the Select Components screen displays details about the errors. Fix any errors, then click **Next** again.

After the checking is complete with no errors, click **OK** to dismiss the dialog box and go to the next screen.

6. Schema Passwords screen

   For each application listed in the **Component** column, enter the same password in the **Schema Password** and **Confirm Password** columns.

   For a development system, you might want to select **Use same passwords for all schemas**, near the top of the screen. Enter your password two times, in the **Password** and **Confirm Password** field.

   > **Note:**   Record all schema passwords from this screen because you will need them later to configure your applications.

   Click **Next**.

7. Map Tablespaces screen

   If you want to create new tablespaces or modify existing ones, click **Manage Tablespaces** and follow the directions on the screen. For more information creating or modifying tablespaces, see "Map Tablespaces Screen" in *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

   Click **Next** on the Map Tablespaces screen. The Validating and Creating Tablespaces dialog box appears.

   If you have any validation errors, the Map Tablespaces screen displays details about the errors. You can track errors in log files, such as `irm.log` and `rcu.log`. This screen displays the log locations. Fix any errors, then click **Next** again. After the tablespaces are created with no errors, click **OK** to dismiss the dialog box.

8. Summary screen

   Click **Create**. The CREATE dialog box.

   If you have any schema creation errors, the Summary screen displays details about the errors. Fix any errors, then click **Next** again.

   After RCU creates the schema or schemas with no errors, click **OK** to dismiss the dialog box.

9. Completion Summary screen

   This screen shows the locations of the RCU log file and component (application) log files.

   Click **Close**.

   > **Note:**   The user account created for a schema has a default expiration date of six months after creation. The database administrator should change the expiration of the user account to a later date. To view the expiration data for an account, use the SQL statement `SELECT * FROM all_users` or `SELECT * FROM dba_users`.

For more information about RCU, see *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

3

Installing Oracle Enterprise Content Management Suite

This chapter explains how to install the Oracle Enterprise Content Management Suite component of Oracle Fusion Middleware.

This chapter includes the following sections:

- Section 3.1, "Preparing for Installation"
- Section 3.2, "Installing Oracle Enterprise Content Management Suite in Oracle Fusion Middleware"

3.1 Preparing for Installation

Before you install Oracle Enterprise Content Management Suite, you need to verify that your system meets the installation requirements and set environment variables. If your system does not have Oracle WebLogic Server installed, you need to install it in a new Middleware home. To provide accessibility on a Windows operating system, you can also install Java Access Bridge.

3.1.1 Meeting System Requirements

Before performing any installation, you should read the system requirements and certification documents to ensure that your environment meets the minimum installation requirements for the products you are installing. Both of these documents are available on Oracle Technology Network (OTN):

- "Oracle Fusion Middleware System Requirements and Specifications" at

  http://www.oracle.com/technology/software/products/ias/files/fusion _requirements.htm

  This document contains information related to hardware and software requirements, minimum disk space and memory requirements, and required system libraries, packages, or patches.

- "Oracle Fusion Middleware Supported System Configurations" at

  http://www.oracle.com/technology/software/products/ias/files/fusion _certification.html

  This document contains information related to supported installation types, platforms, operating systems, databases, JDKs, and third-party products.

> **Note:** For the 32-bit version of the product, the system on which you are installing must be a supported 32-bit system. Installing a 32-bit version of the product on a 64-bit system is not supported.

3.1.2 Installing Oracle WebLogic Server in a Middleware Home

Oracle Enterprise Content Management Suite requires a Middleware home with Oracle WebLogic Server on your system. If your system does not already have Oracle WebLogic Server, you can install it in a new Middleware home directory, before or after installation of the database and creation of the schemas.

To install Oracle WebLogic Server in a Middleware home:

1. Insert the Oracle WebLogic Server DVD, or download the installer from the Oracle E-Delivery Web site at

   http://edelivery.oracle.com/

   You can download one of the following executable files:

   - `wls1032_linux32.bin` (for Linux x86 systems)

   - `wls1032_solaris32.bin` (for 32-bit Solaris systems)

   - `wls1032_win32.exe` (for 32-bit Windows systems)

   - `wls1032_generic.jar` (for all 64-bit systems)

   The 32-bit executable files are bundled with the appropriate JDK version. If you use the 64-bit installer, you will need to invoke the installer with a supported JDK for your platform. This JDK must be installed on your system before you install Oracle WebLogic Server. The JDK must be installed in a directory without spaces in the directory path (not underneath the `/Program Files` directory in a Windows operating system). For a list of supported JDKs for your operating system, see the Oracle Fusion Middleware Supported System Configurations page on Oracle Technology Network at

   http://www.oracle.com/technology/software/products/ias/files/fusion
   _certification.html

2. Either run your installer file directly from the DVD, or copy the file to your local system and run it locally, after considering these notes:

   - Before running the installer on a UNIX operating system that is not Linux, set your system's `DISPLAY` environment variable to a valid X Server.

   - Set the `JAVA_HOME` environment variable to the installation location of the supported JDK you installed for your system.

   - If you are installing Oracle WebLogic Server on a 64-bit system, use the `-d64` flag when using a 32/64-bit hybrid JDK (such as the HP JDK for HP-UX and SUN JDK for Solaris SPARC).

     For a 32/64-bit hybrid JDK, to validate that your `JAVA_HOME` environment variable refers to a 64-bit JDK, execute *JAVA_HOME*`/bin/java -version` (or *JAVA_HOME*`/bin/java -d64 -version`), in which *JAVA_HOME* is the value of the environment variable.

   To run the installer on a 32-bit Linux operating system, use this command:

   ```
   ./wls1032_linux32.bin
   ```

To run the installer on a 32-bit Windows operating system, use this command:

```
wls1032_win32.exe
```

To run the installer on a 64-bit UNIX operating system, use either of these commands:

```
JAVA_HOME/bin/java -jar wls1032_generic.jar
```

```
JAVA_HOME/bin/java -d64 -jar wls1032_generic.jar
```

To run the installer on a 64-bit Windows operating system, use this command:

```
JAVA_HOME\bin\java -jar wls1032_generic.jar
```

3. Welcome screen

   Click **Next**.

4. Choose Middleware Home Directory screen

   Select **Create a new Middleware Home**.

   Specify a location for your new Middleware home directory, which *MW_HOME* represents in path names. If this directory already exists on your system, the directory must be empty. If it does not already exist, then the installer creates it.

   Note: Record this location because you will need to provide it during the installation of Oracle Enterprise Content Management Suite.

   For more information, see "Middleware Home and WebLogic Home Directories" in *Oracle Fusion Middleware Installation Planning Guide*.

   Click **Next**.

5. Register for Security Updates screen

   Select whether or not to receive the latest product and security updates. If you choose not to receive anything, you need to verify your selection.

   Click **Next**.

6. Choose Install Type screen

   Select **Typical**, and click **Next**.

7. Choose Product Installation Directories screen

   Specify a location for your Oracle WebLogic Server home directory, which *WL_HOME* represents in path names. The default location for *WL_HOME* is *MW_HOME*/wlserver_10.3 (UNIX system) or *MW_HOME*\wlserver_10.3 (Windows system). For more information about home directories, see "Middleware Home and WebLogic Home Directories" in *Oracle Fusion Middleware Installation Planning Guide*.

   You can also specify a JDK. To specify a JDK for a 64-bit operating system, you must select **Custom** and the installed 64-bit JDK.

   Click **Next**.

8. Choose Shortcut Location (Windows system only)

   If you are installing on a Windows operating system, you need to specify a location for creating a shortcut to Oracle products.

   Click **Next**.

9. Installation Summary screen

   Click **Next**.

10. Installation Progress screen

    No action is required on this screen.

11. Installation Complete screen

    Deselect **Run Quickstart**.

    Click **Done**.

For more information about installing Oracle WebLogic Server, see *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

3.1.3 Install and Configure Java Access Bridge (Windows System Only)

If you are installing on a Windows operating system, you can install and configure Java Access Bridge for Section 508 Accessibility:

1. Download Java Access Bridge from the Java SE Desktop Accessibility page of the Sun Developer Network at

   http://java.sun.com/javase/technologies/accessibility/accessbridge/

2. Install Java Access Bridge.

3. Copy the `access-bridge.jar` and `jaccess-1_4.jar` files from your installation location to the `jre\lib\ext` directory.

4. Copy the `WindowsAccessBridge.dll`, `JavaAccessBridge.dll`, and `JAWTAccessBridge.dll` files from your installation location to the `jre\bin` directory.

5. Copy the `accessibility.properties` file to the `jre\lib` directory.

For more information about accessibility, see "Using Oracle Fusion Middleware Accessibility Options" in *Oracle Fusion Middleware Administrator's Guide*.

3.1.4 Configure a DHCP Host

If you are installing Oracle Enterprise Content Management Suite on a DHCP host, you must follow the configuration steps in this section for your operating system.

3.1.4.1 Configuring a DHCP Host on a UNIX System

On a UNIX operating system, configure the host to resolve host names to the loopback IP address by modifying the `/etc/hosts` file to contain the following entries:

```
127.0.0.1 hostname.domainname hostname
127.0.0.1 localhost.localdomain localhost
```

To check that the host name resolves to the loopback IP address, ping the domain. For example, on a Linux operating system you could use the following `ping` command:

```
/bin/ping hostname.domainname
```

On a Solaris operating system, you could use the following `ping` command:

```
/usr/sbin/ping hostname.domainname
```

3.1.4.2 Configuring a DHCP Host on a Windows x86 System

On a Windows x86 operating system, install a loopback adapter on the DHCP server (see Section 3.1.4.3, "Installing a Loopback Adapter on a Windows System"). This assigns a local IP address to your computer.

After installing the adapter, add a line immediately after the `localhost` line in the `%SYSTEMROOT%\system32\drivers\etc\hosts` file, with the following format:

```
IP_address    hostname.domainname    hostname
```

Replace `IP_address` with the local IP address of the loopback adapter, `hostname` with the name of the host, and `domainname` with the name of the domain.

3.1.4.3 Installing a Loopback Adapter on a Windows System

On a Windows operating system, you can install a loopback adapter on the DHCP server to assign a local IP address to your computer.

To install a loopback adapter on a Windows system:

1. Open Control Panel.

2. Select **Add Hardware**.

3. In the "Welcome" window, click **Next**.

4. On the "Is the hardware connected?" window, select **Yes, I have already connected the hardware**, then click **Next**.

5. In the "The following hardware is already installed on your computer" window, in the list of installed hardware, select **Add a new hardware device**, then click **Next**.

6. In the "The wizard can help you install other hardware" window, select **Install the hardware that I manually select from a list**, then click **Next**.

7. In the "From the list of hardware types, select the type of hardware you are installing" window, select **Network adapters**, then click **Next**.

8. In the "Select Network Adapter" window, make the following selections:

   - Manufacturer: **Microsoft**

   - Network Adapter: **Microsoft Loopback Adapter**

9. Click **Next**.

10. In the "The wizard is ready to install your hardware" window, click **Next**.

11. In the "Completing the Add Hardware Wizard" window, click **Finish**.

12. Restart your computer.

13. Right-click **My Network Places** on the desktop and choose **Properties**. This displays the Network Connections control panel.

14. Right-click the connection that was just created. This is usually named **Local Area Connection 2**. Choose **Properties**.

15. On the **General** tab, select **Internet Protocol (TCP/IP)**, then click **Properties**.

16. In the Internet Protocol (TCP/IP) Properties dialog box, click **Use the following IP address**, and then do the following steps:

    a. IP Address: Enter a nonroutable IP for the loopback adapter, such as one of the following nonroutable addresses:

    ```
    192.168.x.x (x is any value between 1 and 255)
    10.10.10.10
    ```

    b. Subnet mask: Enter `255.255.255.0`.

    c. Record the values you entered because you will them need later in this procedure.

    d. Leave all other fields empty.

    e. Click **OK**.

17. In the Local Area Connection 2 Properties dialog box, click **OK**.

18. Close the Network Connections control panel.

19. Restart the computer.

3.1.4.4 Removing a Loopback Adapter from a Windows System

You can remove a loopback adapter through Control Panel.

To remove a loopback adapter from a Windows system:

1. Start the System control panel.

   Select **Start > Control Panel > System**.

2. On the **Hardware** tab, click **Device Manager**.

3. In the Device Manager window, expand **Network adapters**. You should see **Microsoft Loopback Adapter**.

4. Right-click **Microsoft Loopback Adapter** and select **Uninstall**.

5. Click **OK**.

3.1.5 Installing on a Non-Networked Computer

You can install Oracle Enterprise Content Management Suite on a non-networked computer, such as a laptop. Because a non-networked computer has no access to other computers, you have to install all the components that you need on the computer.

In addition, you must follow the instructions in Section 3.1.4, "Configure a DHCP Host" to install a loopback adapter and modify the `hosts` file on your system.

3.1.6 Installing on a Multihomed Computer

You can install Oracle Enterprise Content Management Suite on a multihomed computer. A multihomed computer is associated with multiple IP addresses. This is typically achieved by having multiple network cards on the computer. Each IP address is associated with a host name; additionally, you can set up aliases for each host name.

The installer picks up the fully qualified domain name from the first entry in `/etc/hosts` file (UNIX system) or `%SYSTEMROOT%\system32\drivers\etc\hosts` file (Windows system). For example, the installer would pick up myhost1.mycompany.com for configuration if your file contains the following entries:

```
127.0.0.1 localhost.localdomain localhost
10.148.56.76 myhost1.mycompany.com myhost1
10.148.56.77 devhost2.mycompany.com devhost2
```

For specific network configuration of a system component, refer to the individual component's configuration documentation.

3.2 Installing Oracle Enterprise Content Management Suite in Oracle Fusion Middleware

When you install Oracle Enterprise Content Management Suite, you perform a base installation of the following products in an ECM Oracle home directory on your system:

- Oracle Imaging and Process Management (Oracle I/PM)
- Oracle Information Rights Management (Oracle IRM)

After installation, you can deploy either or both of these products to an Oracle WebLogic Server domain, as applications.

> **Note:** For document conversions on a Solaris SPARC platform, Oracle I/PM requires the GNU Compiler Collection (GCC) package 3.4.2 or later in the `/usr/local/packages` directory.
>
> Install this package on the Solaris operating system that will run Oracle I/PM. You can download GCC from the Sunfreeware Web site at
>
> http://www.sunfreeware.com
>
> You also need to set the LD_LIBRARY_PATH environment variable to `/usr/local/packages/gcc-3.4.2/lib` before starting the Oracle I/PM Managed Server. If you are using a later version of GCC, set that version instead of `3.4.2`.

3.2.1 Providing the Location of an Inventory Directory on a UNIX System

If you are installing on a UNIX operating system, and if this is the first time any Oracle product is being installed on your system with the Oracle Universal Installer, you will be asked to provide the location of an inventory directory. This is where the installer will set up subdirectories and maintain inventory data for each Oracle product that is installed on the machine.

To provide the location of an inventory directory on a UNIX system:

1. On the Specify Inventory Directory screen, specify the location of the inventory directory.

    This screen appears only on a UNIX operating system, for the first installation by Oracle Universal Installer. The installer will use the inventory directory to keep track of all Oracle products installed on the machine.

2. Take the action requested in the Inventory Location Confirmation dialog box.

This dialog box asks you to run the *inventory_directory*/createCentralInventory.sh script as the root user.

If you do not have root access on the machine but want to continue with the installation, select **Continue installation with local inventory**.

3.2.2 Creating a Symbolic Link to chmod Command on a Solaris System

Before installing Oracle Enterprise Content Management Suite on a Solaris operating system, you need to create a symbolic link to the chmod command.

To create a symbolic link to the chmod command:

1. Log in as the root user.

2. Execute the following command as root:

```
ln -s /usr/bin/chmod /usr/local/bin/chmod
```

3. Log out, and then log back in with a different user name to start the installation.

Running the installer as the root user is not supported.

3.2.3 Locating Installation Log Files

The location of the installation log file depends on your operating system:

- *USER_HOME*/oraInventory/log/install*date_time* (UNIX directory)

- %PROGRAMFILES%\Oracle\Inventory\logs\install*date_time* (Windows directory)

3.2.4 Installing Oracle Enterprise Content Management Suite

Table 3–1 summarizes the steps for installing Oracle Enterprise Content Management Suite. The procedure following the table provides more detailed instructions.

During the installation, if you need additional help with any of the screens, click the name of the screen in the instructions to see its description in Appendix A, "Oracle Enterprise Content Management Suite Installation Screens," or click **Help** on the screen in the installer to access the online help.

> **Note:** Running the installer as the root user is not supported.

Table 3–1   Installation Procedure for Oracle Enterprise Content Management Suite

Step	Screen	Actions
1	None.	Start the Oracle Enterprise Content Management Suite installer, which is on Disk 1 of the suite's media.
		If you are installing the suite from a ZIP file, you need to unzip the file to a directory. `Disk 1` will be a subdirectory of the suite's media directory.
		On a UNIX operating system:
		`cd ecm_media_loc/Disk1` `./runInstaller [-jreLoc jre_location]`
		On a Windows operating system:
		`cd ecm_installer_loc` `setup.exe [-jreLoc jre_location]`
2	Welcome	Click **Next** to continue.
3	Prerequisite Checks	Click **Next** to continue.
4	Specify Installation Location	Specify the Middleware home (`MW_HOME`) and ECM Oracle home (`ECM_ORACLE_HOME`) locations. The ECM Oracle home directory must be inside the Middleware home directory.
		Click **Next** to continue.
5	Installation Summary	Verify the information on this screen.
		Click **Install** to begin the installation.
6	Installation Progress	When the installation is 100% complete, click **Next** to go to the last screen.
7	Installation Completed	Click **Save** to save the installation configuration, and then click **Finish**.

To install Oracle Enterprise Content Management Suite:

1. Start the Oracle Enterprise Content Management Suite installer.

   This installer requires the location of a Java Runtime Environment (JRE) on your system. A JRE was installed with Oracle Fusion Middleware. The default JRE location for a production environment is *MW_HOME*/`jrockit_160_14_R27.6.5-32/jre` (UNIX directory) or *MW_HOME*\`jrockit_160_14_R27.6.5-32\jre` (Windows directory), where *MW_HOME* is the Middleware home directory. The default JRE location for a development environment is *MW_HOME*/`jdk160_14_R27.6.5-32/jre` (UNIX directory) or *MW_HOME*\`jdk160_14_R27.6.5-32\jre` (Windows directory).

   For a 64-bit installation, you can either use the `-jreLoc` option or allow the installer to prompt for the directory containing `bin/java`.

   To start the installer on a UNIX operating system:

   ```
   cd ecm_media_loc/Disk1
   ./runInstaller [-jreLoc jre_location]
   ```

   Note: Starting the installer as the user `root` is not supported.

To start the installer on a Windows operating system:

```
cd ecm_installer_loc
setup.exe [-jreLoc jre_location]
```

2. On the Welcome screen, click **Next** to begin the installation.

3. On the Prerequisite Checks screen, after the prerequisite checking is complete with no errors, click **Next**.

   If the screen display an error message in the bottom section, fix the error, and then click **Retry** to start the prerequisite checking again. Repeat this until the prerequisite checking is complete with no errors.

   If you want to stop the installation process while you fix a prerequisite error, click **Abort**.

   If you want to ignore an error or warning message and continue with the installation, click **Continue**.

4. On the Specify Installation Location screen, enter values into the following fields, and then click **Next**.

   - **Oracle Middleware Home:** Select the Middleware home directory.

   - **Oracle Home Directory:** Specify the directory where you want to install Oracle Enterprise Content Management Suite.

     If you specify a directory that already exists, it must be empty and inside the Middleware home directory.

     If you specify a new directory, the installer creates it inside the Middleware home directory.

   The installation directory becomes the Oracle home directory for Oracle Enterprise Content Management Suite. Run-time components cannot write to this directory.

   > **Note:** This document refers to this directory as the ECM Oracle home to avoid confusion with the Oracle home directories of other Java components of Oracle Fusion Middleware. For more information, see "Oracle Home and Oracle Common Home Directory" in *Oracle Fusion Middleware Installation Planning Guide*.

5. On the Installation Summary screen, click **Save** if you want to save the response file, and then click **Install** to start the installation.

   If you want to change the configuration, you can return to a previous screen by clicking its name in the navigation tree on the left or **Back**. After you edit the configuration, you can continue the installation from the previous screen.

6. On the Installation Progress screen, you can monitor the progress of your installation.

   If you want to stop the installation, click **Cancel**.

   After the progress reaches 100%, click **Next** to go to the last screen.

7. On the Installation Completed screen, click **Save** if you want to save the installation configuration, and click **Finish** to exit the installer.

4

Configuring Oracle Enterprise Content Management Suite

This chapter explains how to configure an Oracle WebLogic Server domain for Oracle Enterprise Content Management Suite applications.

This chapter includes the following sections:

- Section 4.1, "Preparing to Configure Oracle Enterprise Content Management Suite"
- Section 4.2, "Creating an Oracle WebLogic Server Domain"
- Section 4.3, "Extending an Existing Domain"
- Section 4.4, "Reassociating the Identity Store with an External LDAP Authentication Provider"
- Section 4.5, "Adding Users to Oracle Internet Directory"
- Section 4.6, "Configuring Desktop Authentication"
- Section 4.7, "Configuring Managed Server Clusters"
- Section 4.8, "Migrating a Domain with Pack and Unpack"

4.1 Preparing to Configure Oracle Enterprise Content Management Suite

After you have successfully run the Oracle Fusion Middleware 11*g* Oracle Enterprise Content Management Suite Installer, you can deploy and configure the following Oracle Enterprise Content Management Suite products as applications:

- Oracle Imaging and Process Management
- Oracle Information Rights Management

To configure these applications, you can create or extend an Oracle WebLogic Server domain, which includes a Managed Server for each deployed application and one Administration Server. Each of these servers is an Oracle WebLogic Server instance.

You can create a domain to include either or both of these applications. Or you can create a domain to include a Managed Server for either application (one Managed Server) and then extend the domain with a Managed Server for the other application. For Oracle I/PM, you can extend the domain with Oracle SOA Suite, which includes Oracle BPEL Process Manager.

> **Note:** The Oracle I/PM product deployment provides for up to 10 GB of disk space to be used to stage simultaneous document uploads through the user interface. This limit exists to provide an upper limit to thwart malicious server attacks.

If you have not successfully run the installer on your system, first see Chapter 3, "Installing Oracle Enterprise Content Management Suite."

To create a domain for one or more Oracle Enterprise Content Management Suite applications, follow the instructions in Section 4.2, "Creating an Oracle WebLogic Server Domain."

To extend an existing domain for one or more Oracle Enterprise Content Management Suite applications, follow the instructions in Section 4.3, "Extending an Existing Domain."

During the configuration, if you need additional help with any of the screens, either click the name of the screen in the instructions to see its description in Appendix B, "Oracle Enterprise Content Management Suite Configuration Screens," or click **Help** on the screen in the installer to access the online help.

After you create or extend a domain, you can configure Oracle Enterprise Manager 11*g* Fusion Middleware Control for administration of Oracle Enterprise Content Management Suite applications. Fusion Middleware Control is deployed to the Administration Server when a domain is created. You can use Fusion Middleware Control for additional configuration tasks.

To create a log file of your configuration session, start Fusion Middleware Configuration Wizard with the -log option.

On a UNIX operating system:

```
% ./config.sh -log=log_file_name
```

On a Windows operating system:

```
G:\ config.cmd -log=log_file_name
```

Your log files will be created in your *INVENTORY_HOME*/logs directory.

4.2 Creating an Oracle WebLogic Server Domain

You can create an Oracle WebLogic Server domain for Oracle Enterprise Content Management Suite with Fusion Middleware Configuration Wizard. When you create a domain for the suite, you configure one or more of its applications. The configuration wizard is in the *ECM_ORACLE_HOME*/common/bin directory (UNIX system) or *ECM_ORACLE_HOME*\common\bin directory (Windows system).

ECM_ORACLE_HOME represents the ECM Oracle home directory, where Oracle Enterprise Content Management Suite is installed.

Table 4–1 describes the steps for creating a domain and provides links to descriptions of the screens in Appendix B, "Oracle Enterprise Content Management Suite Configuration Screens."

Table 4–1   Procedure for Creating a New Domain

Step	Screen	When This Screen Appears	Description and Action Required
1	None.	Always	Start Fusion Middleware Configuration Wizard.
			On a UNIX operating system:
			`cd ECM_ORACLE_HOME/common/bin` `./config.sh`
			On a Windows operating system:
			`cd ECM_ORACLE_HOME\common\bin` `config.cmd`
2	Welcome	Always	Select **Create a new WebLogic Domain**.
			Click **Next** to continue.
3	Select Domain Source	Always	Select **Generate a domain configured automatically to support the following products** and either or both of these products:
			■ **Oracle Information Rights Management**
			■ **Oracle Imaging and Process Management**
			When you select **Oracle Imaging and Process Management** or **Oracle Information Rights Management** on the Select Domain Source screen, **Oracle Enterprise Manager** and **Oracle JRF** are automatically selected.
			Click **Next** to continue.
4	Specify Domain Name and Location	Always	Enter the name of the domain you want to create in the **Domain name** field.
			The default location for the domain is *MW_HOME*/user_projects/domains/ (UNIX system) or *MW_HOME*\user_projects\domains\ (Windows system). You can specify a different location in the **Domain location** field.
			Note: Record the domain name and location from this screen because you will need them later to start the Administration Server.
			You can specify the location of the Oracle Enterprise Content Management Suite application in the **Application location** field. The default location is *MW_HOME*/user_projects/applications/.
			Click **Next** to continue.
5	Configure Administrator User Name and Password	Always	The **User name** field has the default administrator user name, `weblogic`. You can specify a different administrator user name.
			In the **User password** field, enter the password for the administrator user.
			Note: Record the administrator user name and password from this screen because you will need them later to start the Administration Server and to access the domain through the Oracle WebLogic Server Administration Console or Oracle Enterprise Manager 11*g* Fusion Middleware Control.
			Click **Next** to continue.

Table 4–1   (Cont.) Procedure for Creating a New Domain

Step	Screen	When This Screen Appears	Description and Action Required
6	Configure Server Start Mode and JDK	Always	Under WebLogic Domain Startup Mode, **Development Mode** is the default mode. For a production system, select **Production Mode**.
			Under JDK Selection, you can leave **Available JDKs** and the default JDK selected, or you can change them. The default JDK for development mode is **Sun SDK 160_14**. The default JDK for production mode is **JRockit SDK 1.6.0_14**. To specify a different JDK, select **Other JDK**, and enter its location.
			Click **Next** to continue.
7	Configure JDBC Component Schema	Always	Configure each component schema, including OWSM MDS Schema if it was created with Repository Creation Utility (RCU), in the following fields:
			■ **Component Schema:** Select a component schema row.
			■ **Vendor:** Select a database vendor from the list.
			■ **Driver:** Leave the default driver for the database vendor selected, or select a driver for the component schema from the list.
			■ **Schema Owner:** Enter the user name of the application schema owner, specified during schema creation with RCU.
			■ **Schema Password:** Enter the schema password, specified during schema creation with RCU.
			■ **DBMS/Service:** Enter the name of the database instance if `Oracle's Driver (Thin) for Instance connections` is selected in the **Driver** field, or enter the service name (global database name) if `Oracle's Driver (Thin) for Service connections` is selected in the **Driver** field. For Microsoft SQL Server, you must enter a database name because there is no service name.
			Specify the database that contains the application schema or schemas.
			For Oracle RAC databases, specify the service name of one of the nodes in this field. For example: `sales.example.com`.
			■ **Host Name:** Specify the name of the machine on which your database resides, in the format `host.example.com`. For Oracle RAC databases, specify the Virtual IP name or one of the node names as the host name.
			■ **Listen Port:** Specify the database listen port number. The default port number for an Oracle Database instance is `1521`. The default port number for Microsoft SQL Server is `1433`.
			Click **Next** to continue.

Table 4–1 (Cont.) Procedure for Creating a New Domain

Step	Screen	When This Screen Appears	Description and Action Required
8	Test Component Schema	Always	The configuration wizard automatically tests the connection to the JDBC component schema.
			If the test fails, click **Previous** to correct the component schema information, and then click **Next** to retest the connection.
			After the test succeeds, click **Next** to continue.
9	Select Optional Configuration	Always	Optionally, select any or all of these options for configuring the Administration Server and Managed Servers:
			■ **Administration Server**
			■ **Managed Servers, Clusters and Machines**
			■ **Deployments and Services**
			■ **RDBMS Security Store**
			Click **Next** to continue to the configuration screens for the selected option or if you did not select any options, to the Configuration Summary screen.
10	Configure the Administration Server	If you selected **Administration Server** on the Select Optional Configuration screen.	The default listen port number for the Administration Server is 7001, which you can change.
			If you want to change the configuration of SSL for the Administration Server, you can select **SSL enabled**. The SSL port is set to 7002 by default in the **SSL Listen Port** field. If **SSL enabled** is selected, you can change the SSL listen port value.
			Click **Next** to continue.
11	Configure Managed Servers	If you selected **Managed Servers, Clusters and Machines** on the Select Optional Configuration screen.	Each Managed Server needs a unique listen port number. For each Managed Server, you can use the default **Listen port** value. For increased security, you can specify a nondefault port number.
			Table 4–2 lists the default port values for the Managed Servers that run Oracle Enterprise Content Management Suite applications.
			If you want to change the SSL configuration for a Managed Server, you can select **SSL enabled** and set or change the **SSL listen port** value.
			For Oracle IRM, SSL is enabled by default, with port number 16101. SSL needs to be enabled so that Oracle IRM Desktop does not show prompts to accept certificates when it contacts the Managed Server. The certificate used must be trusted by Microsoft Internet Explorer on computers running Oracle IRM Desktop.
			Click **Next** to continue.
12	Configure Clusters	If you selected **Managed Servers, Clusters and Machines** on the Select Optional Configuration screen.	Optionally, configure one or more clusters.
			Click **Next** to continue.

Table 4–1 (Cont.) Procedure for Creating a New Domain

Step	Screen	When This Screen Appears	Description and Action Required
13	Configure Machines	If you selected **Managed Servers, Clusters and Machines** on the Select Optional Configuration screen.	Optionally, configure machines to host Oracle WebLogic Server. Click **Next** to continue.
14	Target Deployments to Clusters or Servers	If you selected **Deployments and Services** on the Select Optional Configuration screen.	Optionally, assign each Managed Server to a cluster. Oracle IRM should be deployed on a cluster or on a managed server that is not a member of any cluster because Oracle IRM uses `persistent-store-type` as `replicated_if_clustered`. If the Oracle IRM Web application is deployed on a clustered server, the in-effect `persistent-store-type` will be replicated. Otherwise, `memory` is the default. Make sure that the Oracle IRM application is not deployed to one of the servers in a cluster. Click **Next** to continue.
15	Target Services to Clusters or Servers	If you selected **Deployments and Services** on the Select Optional Configuration.	Optionally, modify how your services are targeted to servers or clusters. If OWSM MDS Schema was created with RCU, target it to the Administration Server by selecting **AdminServer** on the left and **mds-owsm** under **JDBC** and **JDBC System Resource** on the right. Click **Next** to continue.
16	Configure RDBMS Security Store Database	If you selected **RDBMS Security Store** on the Select Optional Configuration screen.	Optionally, make changes to your RDBMS security store. Click **Next** to continue.
17	Configuration Summary	Always	Review your configuration and make any corrections or updates by following the instructions on the screen. You can click **Previous** on each screen to go back to a screen where you want to change the configuration. When the configuration is satisfactory, click **Create** to create the domain.
18	Creating Domain	Always	When the domain is created successfully, click **Done**.

Table 4–2 lists the default port values for the Managed Servers that run Oracle Enterprise Content Management Suite applications.

Table 4–2 Default Ports for Managed Servers

Managed Server	Default Listen Port	Default SSL Port	Port Range
Oracle I/PM	16000	16001	16000-16099
Oracle IRM	16100	16101	16100-16199

The following operations should have completed successfully:

- Creation of an Oracle WebLogic Server domain, with an Administration Server

- Creation of a Managed Server for each application that you selected on the Select Domain Source screen

- Deployment of each application to its Managed Server

  An application is not active until its Managed Server is started. For more information, see Section 7.2, "Starting Managed Servers."

4.3 Extending an Existing Domain

You can extend an existing Oracle WebLogic Server domain to configure one or more Oracle Enterprise Content Management Suite applications. Fusion Middleware Configuration Wizard is in the *ECM_ORACLE_HOME*/common/bin directory (UNIX system) or *ECM_ORACLE_HOME*\common\bin directory (Windows system).

You can also extend a domain to include other applications in the same domain. For example, you could extend an Oracle WebCenter domain to include an Oracle IRM Managed Server. Or you could extend an Oracle I/PM domain to include Oracle SOA Suite.

> **Note:** Before you extend a domain to include Oracle SOA Suite on an AIX platform, you need to confirm that the soa-ibm-addon.jar file is in the *SOA_ORACLE_HOME*/soa/modules directory. Make sure that the file is there, and add the following entry to the *SOA_ORACLE_HOME*/bin/ant-sca-compile.xml file at line 65:
>
> ```
>  <include name="soa-ibm-addon.jar"/>
> ```

Table 4–3 describes the steps for extending a domain and provides links to descriptions of the screens in Appendix B, "Oracle Enterprise Content Management Suite Configuration Screens."

Table 4–3   Procedure for Extending an Existing Domain

Step	Screen	When This Screen Appears	Description and Action Required
1	None.	Always	Start Fusion Middleware Configuration Wizard. On a UNIX operating system: cd *ECM_ORACLE_HOME*/common/bin ./config.sh On a Windows operating system: cd *ECM_ORACLE_HOME*\common\bin config.cmd
2	Welcome	Always	Select **Extend an existing WebLogic Domain**. Click **Next** to continue.
3	Select a WebLogic Domain Directory	Always	Select the Oracle WebLogic Server directory to which you want to add your applications or services, or both. Click **Next** to continue.

Table 4–3   (Cont.) Procedure for Extending an Existing Domain

Step	Screen	When This Screen Appears	Description and Action Required
4	Select Extension Source	Always	Select **Extend my domain automatically to support the following added products** and either or both of these products:
			■ **Oracle Information Rights Management**
			■ **Oracle Imaging and Process Management**
			When you select **Oracle Imaging and Process Management** or **Oracle Information Rights Management** on the Select Domain Source screen, **Oracle Enterprise Manager** and **Oracle JRF** are automatically selected.
			Click **Next** to continue.
5	Configure JDBC Component Schema	Always	Configure each component schema, including OWSM MDS Schema if it was created with Repository Creation Utility (RCU), in the following fields:
			■ **Component Schema:** Select a component schema row.
			■ **Vendor:** Select a database vendor from the list.
			■ **Driver:** Leave the default driver for the database vendor selected, or select a driver for the component schema from the list.
			■ **Schema Owner:** Enter the user name of the application schema owner, specified during schema creation with Repository Creation Utility (RCU).
			■ **Schema Password:** Enter the schema password, specified during schema creation with RCU.
			■ **DBMS/Service:** Enter the name of the database instance if `Oracle's Driver (Thin) for Instance connections` is selected in the **Driver** field, or enter the service name (global database name) if `Oracle's Driver (Thin) for Service connections` is selected in the **Driver** field. For SQL Server, you must enter a database name because there is no service name.
			Specify the database that contains the application schema or schemas.
			For Oracle RAC databases, specify the service name of one of the nodes in this field. For example: `sales.example.com`.
			■ **Host Name:** Specify the name of the machine on which your database resides, in the format `host.example.com`. For Oracle RAC databases, specify the Virtual IP name or one of the node names as the host name.
			■ **Listen Port:** Specify the database listen port number. The default port number for an Oracle Database instance is `1521`. The default port number for SQL Server is `1433`.
			Click **Next** to continue.

Table 4–3   (Cont.) Procedure for Extending an Existing Domain

Step	Screen	When This Screen Appears	Description and Action Required
6	Test Component Schema	Always	The configuration wizard automatically tests the connection to the JDBC component schema.
			If the test fails, click **Previous** to correct the component schema information, and then click **Next** to retest the connection.
			After the test succeeds, click **Next** to continue.
7	Select Optional Configuration	Always	Optionally, select any or all of these options for configuring Managed Servers:
			■ **Managed Servers, Clusters and Machines**
			■ **Deployments and Services**
			■ **JMS File Store**
			Click **Next** to continue to the configuration screens for the selected option or if you did not select any options, to the Configuration Summary screen.
8	Configure Managed Servers	If you selected **Managed Servers, Clusters and Machines** on the Select Optional Configuration screen.	Each Managed Server needs a unique listen port number. For each Managed Server, you can use the default **Listen port** value or, for increased security, specify a nondefault port number.
			Table 4–2 lists the default port values for the Managed Servers that run Oracle Enterprise Content Management Suite applications.
			To change the SSL configuration for a Managed Server, you can select **SSL enabled** and set or change the **SSL listen port** value.
			For Oracle IRM, SSL is enabled by default, with port number 16101. SSL needs to be enabled so that Oracle IRM Desktop does not show prompts to accept certificates when it contacts the Managed Server. The certificate used must be trusted by Microsoft Internet Explorer on computers running Oracle IRM Desktop.
			Click **Next** to continue.
9	Configure Clusters	If you selected **Managed Servers, Clusters and Machines** on the Select Optional Configuration screen.	Optionally, change the cluster configuration.
			Click **Next** to continue.
10	Configure Machines	If you selected **Managed Servers, Clusters and Machines** on the Select Optional Configuration screen.	Optionally, configure machines to host Oracle WebLogic Server.
			Click **Next** to continue.

Table 4–3   (Cont.) Procedure for Extending an Existing Domain

Step	Screen	When This Screen Appears	Description and Action Required
11	Target Deployments to Clusters or Servers	If you selected **Managed Servers, Clusters and Machines** on the Select Optional Configuration screen.	Optionally, assign each Managed Server to a cluster.
			Oracle IRM should be deployed on a cluster or on a managed server that is not a member of any cluster because Oracle IRM uses `persistent-store-type` as `replicated_if_clustered`. If the Oracle IRM Web application is deployed on a clustered server, the in-effect `persistent-store-type` will be replicated. Otherwise, `memory` is the default.
			Make sure that the Oracle IRM application is not deployed to one of the servers in a cluster.
			Click **Next** to continue.
12	Target Services to Clusters or Servers	If you selected **Deployments and Services** on the Select Optional Configuration.	Optionally, modify how your services are targeted to servers or clusters.
			If OWSM MDS Schema was created with RCU, target it to the Administration Server by selecting **AdminServer** on the left and **mds-owsm** under **JDBC** and **JDBC System Resource** on the right.
			Click **Next** to continue.
13	Configuration Summary	Always.	When the configuration is satisfactory, click **Extend** to extend the domain.
14	Creating Domain (Extended Domain)	Always	When the domain is successfully extended, click **Done**.

The following operations should have completed successfully:

- Extension of an existing Oracle WebLogic Server domain to include the application or applications that you selected on the Extend Domain Source screen

- Creation of a Managed Server for each application that you selected

- Deployment of each application to its Managed Server

  An application is not active until its Managed Server is started. For more information, see Section 7.2, "Starting Managed Servers."

4.4 Reassociating the Identity Store with an External LDAP Authentication Provider

In a production system, Oracle Enterprise Content Management Suite applications need to use an external Lightweight Directory Application Protocol (LDAP) authentication provider rather than the Oracle WebLogic Server embedded LDAP server, which is part of the default configuration. You need to reassociate the identity store for your application with one of the following external LDAP authentication providers before you complete the configuration of a Managed Server and before you connect a Managed Server to a repository:

- Oracle Internet Directory

- Oracle Virtual Directory

- Third-party LDAP server

The user who logs in first to an Oracle I/PM Managed Server is provisioned with full security throughout the server. It is easier to reassociate the identity store for Oracle

I/PM with an external LDAP authentication provider before the first user logs in completes the configuration of the Oracle I/PM Managed Server, and connects it to the Oracle Universal Content Management (Oracle UCM) repository.

The Oracle IRM domain, which is different from the Oracle WebLogic Server domain, gets created the first time a user logs in to the Oracle IRM Management Console. The first user who logs in to the console with the WebLogic Administrator role is made the Domain Administrator for the Oracle IRM instance. Before you migrate user data for Oracle IRM, the users need to be in the target LDAP identity store. The general process for reassociating Oracle IRM users and migrating data follows:

1. Back up existing data with the `preIRMUserStoreUpgrade` script.

2. Reassociate the identity store with an external LDAP directory.

3. Verify that all users and groups exist in target LDAP identity store.

4. Migrate data with the `postIRMUserStoreUpgrade` script.

You can reassociate the identity store for an Oracle WebLogic Server domain with Oracle Internet Directory and migrate Oracle I/PM or Oracle IRM users from the embedded LDAP directory to Oracle Internet Directory. The following procedure describes how to reassociate the identity store with Oracle Internet Directory.

You can use a similar procedure to reassociate the identity store with other LDAP authentication providers. Each provider has a specific authenticator type, and only that type should be configured. Table 4–4 lists the available authenticator types.

Table 4–4   LDAP Authenticator Types

LDAP Authentication Provider	Authenticator Type
Microsoft AD	ActiveDirectoryAuthenticator
SunOne LDAP	IPlanetAuthenticator
Oracle Internet Directory	OracleInternetDirectoryAuthenticator
Oracle Virtual Directory	OracleVirtualDirectoryAuthenticator
EDIRECTORY	NovellAuthenticator
OpenLDAP	OpenLDAPAuthenticator
EmbeddedLDAP	DefaultAuthenticator

To reassociate the identity store with an external LDAP authentication provider:

1. Create the same Administration user in Oracle Internet Directory that was created during configuration of the domain that includes the Managed Server for your application; for example, `weblogic`.

   For optional user attributes, set the `userPassword` and `user name` attributes to whatever you configured for the domain Administration user name. For example, if `uid` was configured as a user name attribute, then you would need to set the same value for the `uid` attribute in Oracle Internet Directory.

2. Enter the same password for the Oracle Internet Directory user that was specified for the corresponding domain user.

3. If a user with the Administrator role has already logged into the Oracle IRM Management Console, before switching over to a new identity store, run `preIRMUserStoreUpgrade()` to back up the User information, as follows:

```
cd ECM_ORACLE_HOME/common/bin
./wlst.sh
wls:/offline>
connect('weblogic','password','t3://managedServerHost:ManagedServerPort')
Connecting to t3://managedServerHost:ManagedServerPort with userid weblogic ...
Successfully connected to managed Server 'IRM_server1' that belongs to domain
'base_domain'.
wls:/base_domain/serverConfig> preIRMUserStoreUpgrade()
Enter Server URL: t3://managedServerHost:ManagedServerPort
Enter Username: weblogic
Enter Password:
Connecting to server...
No. of accounts retrieved so far: 1
Done!
wls:/base_domain/serverConfig> exit()
```

4. Configure the Oracle Internet Directory authentication provider:

a. Start the Administration Server for your Oracle WebLogic Server domain, as described in Section 7.1, "Starting the Administration Server."

b. Log in to the Administration Console as the domain Administration user, at this URL:

```
http://adminServerHost:adminServerPort/console
```

For `adminServerHost`, specify the name of the computer that hosts the Administration Server for your domain. For `adminServerPort`, specify the listen port number for the Administration Server. The default number is `7001`. For example:

```
http://myHost:7001/console
```

To log in, supply the user name and password that were specified on the Configure Administrator User Name and Password screen in the configuration wizard.

c. Under Domain Structure on the left, select **Security Realms**.

d. In the Realms table on the Summary of Security Realms page, click **myrealm** in the **Name** column to open the Settings for myrealm page.

e. Click the **Providers** tab, and then click **New** under the Authentication Providers table on the **Authentication** tab.

f. In the Create a new Authentication Provider dialog box, enter a provider name in the **Name** field, change the type to `OracleInternetDirectoryAuthenticator`, and then click **OK**.

For a list of authenticator types for different LDAP Authentication Providers, see Table 4–4.

g. In the Authentication Providers table, click **Reorder**, move the provider you just created to the top of the list, and then click **OK**.

h. Click **DefaultAuthenticator**, change the **Control Flag** value to `OPTIONAL`, and then click **Save**.

i. Go back to the **Providers** tab.

j. Click the name of the authentication provider you just created to navigate to the **Configuration** tab for the provider.

For Oracle IRM, do not change the **Control Flag** value until you have verified that the Oracle Internet Directory configuration is valid.

For Oracle I/PM, change the **Control Flag** value to SUFFICIENT, and then click **Save**.

SUFFICIENT means that if a user can be authenticated against Oracle Internet Directory, no further authentication is processed.

REQUIRED means that the authentication provider must succeed even if another provider already authenticated the user. If the embedded LDAP has been set to OPTIONAL and Oracle Internet Directory has been set to REQUIRED, the embedded LDAP user is no longer valid.

k. Click the **Provider Specific** tab.

Set Provider Specific values in the following fields, and leave default values in the other fields:

* **Host:** The host name or IP address of the LDAP server.

* **Port:** The Oracle Internet Directory Port, 389 by default.

* **Principal:** The Distinguished Name (DN) of the LDAP user that Oracle WebLogic Server should use to connect to the LDAP server; for example:

  cn=orcladmin

* **Credential:** The credential used to connect to the LDAP server (usually a password).

* **Confirm Credential:** The same value as for the **Credential** field.

* **User Base DN:** The base distinguished name (DN) of the tree in the LDAP directory that contains users; for example:

  cn=users,dc=example,dc=com

  In Oracle Internet Directory, this is the value of the **User Search Base** attribute, which you can look up in the OIDDAS administration dialog.

Note: Use an exact DN rather than a top-level DN. Using a top-level DN would provide access to all the default users and groups under the DN, giving access to more users than required by an Oracle IRM or Oracle I/PM application.

---

* **Use Retrieved User Name as Principal:** Specifies whether or not the user name retrieved from the LDAP server should be used as the Principal value.

  Select this attribute for Oracle IRM.

* **Group Base DN:** The base distinguished name (DN) of the tree in the LDAP directory that contains groups; for example:

  cn=groups,dc=example,dc=com

  In Oracle Internet Directory, this is the value of the **Group Search Base** attribute, which you can look up in the OIDDAS administration dialog.

> **Note:** Use an exact DN rather than a top-level DN. Using a top-level DN would provide access to all the default users and groups under the DN, giving access to more users than required by an Oracle IRM or Oracle I/PM application.

* **Propagate Cause For Login Exception:** Propagates exceptions thrown by Oracle Internet Directory, like password expired exceptions, to Oracle WebLogic Server so they show in the console and the logs.

  Select this attribute for Oracle IRM, in the General area of the tab.

If you modify a user name attribute to something other than the default value set for the LDAP server in the authenticator, you must also edit the `jps-config.xml` file to correspond to the modified value. Specifically, you need to add the `username.attr` and `user.login.attr` properties, shown in the following example, for user lookups to function correctly.

```
<!-- JPS WLS LDAP Identity Store Service Instance -->
<serviceInstance name="idstore.ldap" provider="idstore.ldap.provider">
<property name="idstore.config.provider"
value="oracle.security.jps.wls.internal.idstore.WlsLdapIdStoreConfigProvide
r"/>
<property name="username.attr" value="uid"/>
<property name="user.login.attr" value="uid"/>
</serviceInstance>
```

  l. Click **Save**.

5. Shut down the Administration Server, and then restart it to activate the changes.

> **Note:** Authentication providers in an Oracle WebLogic Server domain are chained. This means that user authentication needs to run successfully through all authentication providers. With the **Control Flag** value set to `OPTIONAL` for the default provider, it is allowed to fail without a server startup or user authentication failure.

6. After the server is up again, log in to the Administration Console again, and click **Security Realms** under Domain Structure.

7. In the Realms table on the Summary of Security Realms page, click **myrealm** in the **Name** column to open the Settings for myrealm page.

8. Click the **Providers** tab, then click the **Users and Groups** tab to see a list of users contained in the configured authentication providers, on the **Users** tab, and then click the **Groups** tab to see a list of groups.

   You should see user names from the Oracle Internet Directory configuration, which implicitly verifies that the configuration is working.

9. Check that you have switched the security provider successfully, with either or both of these basic tests:

   ■ After the creation of the new security provider is complete, verify that all the users in that security provider are listed in that same user-group presentation as the list from Step 3.

   ■ Access the Managed Server URL, and log in as any of the Oracle Internet Directory users.

For information about accessing a Managed Server, see Section 7.2, "Starting Managed Servers."

10. For Oracle IRM, if the Oracle Internet Directory instance is configured successfully, change the **Control Flag** value to SUFFICIENT, and then click **Save**.

SUFFICIENT means that if a user can be authenticated against Oracle Internet Directory, no further authentication is processed.

REQUIRED means that the authentication provider must succeed even if another provider already authenticated the user. If the embedded LDAP has been set to OPTIONAL and Oracle Internet Directory has been set to REQUIRED, the embedded LDAP user is no longer valid.

11. For Oracle IRM, restart the Administration Server and the Managed Server.

12. For Oracle IRM, if a user with the Administrator role has already logged into the Management Console, run postIRMUserStoreUpgrade() to update the user information in the Oracle IRM database with new GUIDs, as follows:

```
wls:/offline>
connect('weblogic','password','t3://managedServerHost:managedServerPort')
Connecting to t3://hostname:port with userid weblogic ...
Successfully connected to managed Server 'IRM_server1' that belongs to domain
'base_domain'.
wls:/base_domain/serverConfig> postIRMUserStoreUpgrade()
Enter Server URL: t3://managedServerHost:ManagedServerPort
Enter Username: weblogic
Enter Password:
Connecting to server...
Migrating account name: weblogic
Migration Succeeded
.
Migration Summary
-----------------
Total number of accounts: 1
No. of accounts migrated: 1
No. of failures: 0
```

After the reassociation of the identity store, users in Oracle Internet Directory have the same rights that their namesakes had in the Oracle WebLogic Server embedded LDAP server before the migration of user data. For example, if a user existed in the embedded LDAP server before the migration with the user name weblogic and an Oracle IRM role of Domain Administrator, then after migration the user in Oracle Internet Directory with the user name weblogic would have the Oracle IRM role of Domain Administrator.

4.5 Adding Users to Oracle Internet Directory

You can add users to Oracle Internet Directory with Oracle Directory Services Manager, which is part of Oracle Identity Management. To add an entry to the directory with Oracle Directory Services Manager, you must have write access to the parent entry, and you must know the Distinguished Name (DN) to use for the new entry.

> **Note:** When you add or modify an entry, the Oracle directory server does not verify the syntax of the attribute values in the entry.

For information about adding a group entry, see "Managing Dynamic and Static Groups" in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*. For more information about entries, see "Managing Directory Entries" in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

To add users to Oracle Internet Directory:

1. Invoke Oracle Directory Services Manager and connect to the Oracle Internet Directory server.

2. From the task selection bar, select **Data Browser**.

3. On the toolbar, select the **Create a new entry** icon. Alternatively, right-click any entry and choose **Create**.

   The Create New Entry wizard starts.

4. Specify the object classes for the new entry.

   To select object class entries, click the **Add** icon and use the Add Object Class dialog box. Optionally, use the search box to filter the list of object classes. To add the object class, select it, and then click **OK**. (All the superclasses from this object class through top are also added.)

   > **Note:** You must assign user entries to the inetOrgPerson object class for the entries to appear in the Oracle Internet Directory Self-Service Console in Oracle Delegated Administration Services.

5. In the **Parent of the entry** field, you can specify the full DN of the parent entry for the entry you are creating.

   You can also click **Browse** to locate and select the DN of the parent for the entry you want to add. If you leave the **Parent of the entry** field blank, the entry is created under the root entry.

6. Click **Next**.

7. Choose an attribute that will be the **Relative Distinguished Name** (RDN) value for this entry and enter a value for that attribute.

   You must enter values for attributes that are required for the object class you are using, even if none of them is the RDN value. For example, for object class inetorgperson, attributes cn (common name) and sn (surname or last name) are required, even if neither of them is the RDN value.

8. Click **Next**.

   The wizard displays the next page. (Alternatively, you can click **Back** to return to the previous page.)

9. Click **Finish**.

10. To manage optional attributes, navigate to the entry you have just created in the Data Tree.

11. If the entry is a person, click the **Person** tab and use it to manage basic user attributes.

    Click **Apply** to save your changes or **Revert** to discard them.

    If the entry is a group, see "Managing Dynamic and Static Groups" in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* for instructions.

12. If this is a person entry, you can upload a photograph.

   To upload a photograph, click **Browse**, navigate to the photograph, then click **Open**.

   To update the photograph, click **Update** and follow the same procedure.

   To delete the photograph, click the **Delete** icon.

13. Click **Apply** to save your changes or **Revert** to discard them.

4.6 Configuring Desktop Authentication

You can configure single sign-on (SSO), Oracle Access Manager (OAM), SAML with single sign-on (SSO), and Windows Native Authentication.

For an overview of SSO, see "Configuring Single Sign-On in Oracle Fusion Middleware" in *Oracle Fusion Middleware Security Guide*.

For an overview of Oracle WebLogic Server authentication providers, see "Configuring Authentication Providers" in *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

4.6.1 Configuring Oracle Access Manager

Oracle Access Manager enables users to seamlessly gain access to Web applications and other IT resources across your enterprise. OAM provides a centralized and automated single sign-on (SSO) solution, which includes an extensible set of authentication methods and the ability to define workflows around them. OAM also contains an authorization engine, which grants or denies access to particular resources based on properties of the user requesting access as well as on the environment from which the request was made. Comprehensive policy management, auditing, and integration with other components of your IT infrastructure enrich this core functionality.

For more information about Oracle Access Manager, see "Deploying the Oracle Access Manager Solutions" in *Oracle Fusion Middleware Security Guide*.

4.6.2 Configuring SAML with SSO

To configure the Oracle WebLogic Server SAML authentication provider with SSO for Oracle IRM to share authentication with Oracle I/PM, you need to move the Assertion consumer service (ACS) inside Oracle IRM. Specify *contextRoot*`/samlacs/acs` (for example, `/irm_rights/samlacs/acs`),

instead of simply `/samlacs/acs`, as the ACS URI when configuring the destination site federation services and the Relying Party on the source site.

SSO authentication enables users to log in once and seamlessly navigate between applications without having to log in to each application separately. For information about LDAP and SSO configuration, see "Managing Security" in *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter*.

For SAML configuration information, see "Configuring the SAML Authentication Provider" in *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

4.6.3 Configuring Windows Native Authentication

For information about configuring Windows Native Authentication (Kerberos), see "Configuring a Windows NT Authentication Provider" in *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

4.7 Configuring Managed Server Clusters

For production environments that require increased application performance, throughput, or high availability, you can configure two or more Managed Servers to operate as a cluster. A **cluster** is a collection of multiple Oracle WebLogic Server server instances running simultaneously and working together to provide increased scalability and reliability. In a cluster, most resources and services are deployed identically to each Managed Server (as opposed to a single Managed Server), enabling failover and load balancing. A single domain can contain multiple Oracle WebLogic Server clusters, as well as multiple Managed Servers that are not configured as clusters. The key difference between clustered and nonclustered Managed Servers is support for failover and load balancing. These features are available only in a cluster of Managed Servers.

For an overview of clusters, see "Understanding WebLogic Server Clustering" in *Oracle Fusion Middleware Using Clusters for Oracle WebLogic Server*.

If you select **Managed Servers, Clusters, and Machines** on the Select Optional Configuration screen, you will see the screens described in Table 4–5.

Table 4–5   Managed Servers, Clusters, and Machines Advanced Settings Screens

No.	Screen	Description and Action Required
1	Configure Managed Servers	Add new managed servers, or edit and delete existing managed servers.
		Click **Next** to continue.
2	Configure Clusters	Create clusters if you are installing in a high availability environment. For more information, refer to *Oracle Fusion Middleware High Availability Guide*.
		Click **Next** to continue.
5	Configure Machines	Configure the machines that will host the managed servers.
		Click **Next** to continue.
3	Target Deployments to Clusters or Servers	Assign your managed servers to clusters or servers in your domain.
		Click **Next** to continue.
4	Target Services to Clusters or Servers	Use this screen to target your services (such as JMS and JDBC) to servers or clusters so that your applications can use the services.
		Click **Next** to continue.

You can add a Managed Server to a cluster later, with the Administration Console or Fusion Middleware Control. For more information, see "Scaling Your Environment" in *Oracle Fusion Middleware Administrator's Guide*.

4.8 Migrating a Domain with Pack and Unpack

When an Oracle IRM domain is created, the `weblogic` user is made the domain administrator. A relation is created in the Oracle IRM database schema for the user GUID.

When a second domain is created with `pack` and `unpack`, users need to be migrated with Oracle IRM user migration commands. After the new domain is created, the GUIDs of the users change in the Oracle WebLogic Server embedded LDAP server, but

the Oracle IRM schema still contains the old GUIDs. You have to use user migration commands synch up the new GUIDs (for the second domain).

User migration should be performed for any additional Oracle IRM domains created using same database schema. With the embedded LDAP server, only one of the domains that share the schema can be active at a time. More than one active domain can share a schema if you reassociate the first domain with an external LDAP authentication provider, as described in Section 4.4, "Reassociating the Identity Store with an External LDAP Authentication Provider," and then point each additional domain to the external LDAP authentication provider.

> **Note:** Before packing and unpacking an Oracle IRM domain, you need to configure a key store. For more information, see Section 6.1.2, "Configuring a Key Store for Oracle IRM."

To migrate an Oracle IRM domain with Pack and Unpack:

1. Run Fusion Middleware Configuration Wizard to create an Oracle WebLogic Server domain with Oracle IRM deployed to a Managed Server, as described in Section 4.2, "Creating an Oracle WebLogic Server Domain."

2. Reassociate the identity store of the domain with an external LDAP, as described in Section 4.4, "Reassociating the Identity Store with an External LDAP Authentication Provider."

3. Navigate to the `bin` directory under the `common` directory in the ECM Oracle home.

   - UNIX operating system: *MW_HOME*/*ECM_ORACLE_HOME*/common/bin

   - Windows operating system: *MW_HOME**ECM_ORACLE_HOME*\\common\\bin

4. Before creating a second domain, run the `preIRMUserStoreUpgrade()` script to back up the user information, as follows:

```
preIRMUserStoreUpgrade()

wls:/offline> connect()
Please enter your username [weblogic] :weblogic
Please enter your password [weblogic] :
Please enter your server URL [t3://localhost:7001]
:t3://host:7210
Connecting to t3://host:7210 with userid weblogic ...
Successfully connected to managed Server 'IRM_server1' that belongs to domain
'base_domain4'.

@Warning: An insecure protocol was used to connect to the
server. To ensure on-the-wire security, the SSL port or
Admin port should be used instead.

wls:/base_domain4/serverConfig> preIRMUserStoreUpgrade()
Enter Server URL: t3://host:7210
Enter Username: weblogic
Enter Password:
Connecting to server...
No. of accounts retrieved so far: 1
Done!
wls:/base_domain4/serverConfig> exit()
```

5. Pack `base_domain4`, as in the following UNIX example:

```
./pack.sh -domain=$MW_HOME/user_projects/domains/base_domain4
-template=$MW_HOME/user_projects/templates/base_domain4.jar
-template_name="IRM DOMAIN TEMPLATE" -template_author="name"
-template_desc="IRM Domain" -managed="false"
-log=$MW_HOME/user_projects/templates/pack_base_domain4.log
-log_priority=debug
```

6. Create a second domain by unpacking the file created in the preceding step (`base_domain4.jar`); for example:

```
./unpack.sh -template=$MW_HOME/user_projects/templates/base_domain4.jar
@ -domain=$MW_HOME/user_projects/domains/base_domain5
@ -app_dir=$MW_HOME/user_projects/applications/base_domain5
@ -log=$MW_HOME/user_projects/templates/base_domain5.log
```

7. Stop the Administration Server and Oracle IRM Managed Server in the first domain (`base_domain4`,) as described in Section 8.2, "Stopping Oracle Fusion Middleware Server and Processes."

8. Start the Administration Server and Oracle IRM Managed Server in the second domain (`base_domain5`).

9. Connect to the Oracle IRM Managed Server in the second domain, and run the `postIRMUserStoreUpgrade()` script to update the user information in the Oracle IRM database schema with the new GUIDs, as follows:

```
postIRMUserStoreUpgrade()

wls:/offline> connect()
Please enter your username [weblogic] :weblogic
Please enter your password [weblogic] :
Please enter your server URL [t3://localhost:7001]
:t3://host:7210
Connecting to t3://host:7210 with userid weblogic ...
Successfully connected to managed Server 'IRM_server1' that belongs to domain
'base_domain5'.

Warning: An insecure protocol was used to connect to the
server. To ensure on-the-wire security, the SSL port or
Admin port should be used instead.

wls:/base_domain5/serverConfig> postIRMUserStoreUpgrade()
Enter Server URL: t3://host:7210
Enter Username: weblogic
Enter Password:
Connecting to server...
Migrating account name: weblogic
Migration Succeeded

Migration Summary
-----------------
Total number of accounts: 1
No. of accounts migrated: 1
No. of failures: 0
```

10. Configure the Oracle Internet Directory authentication provider:

   a. Start the Administration Server for your Oracle WebLogic Server domain, as described in Section 7.1, "Starting the Administration Server."

   b. Log in to the Administration Console as the domain Administration user, at this URL:

   ```
   http://adminServerHost:adminServerPort/console
   ```

   For `adminServerHost`, specify the name of the computer that hosts the Administration Server for your domain. For `adminServerPort`, specify the listen port number for the Administration Server. The default number is `7001`. For example:

   ```
   http://myHost:7001/console
   ```

   To log in, supply the user name and password that were specified on the Configure Administrator User Name and Password screen in the configuration wizard.

   c. Under Domain Structure on the left, select **Security Realms**.

   d. In the Realms table on the Summary of Security Realms page, click **myrealm** in the **Name** column to open the Settings for myrealm page.

   e. Click the **Providers** tab, and then click the name of the external LDAP authentication provider in the Authentication Providers table on the **Authentication** tab.

   f. Click **Save**.

11. Restart the Oracle IRM Managed Server.

12. Access the Managed Server URL of the unpacked domain (`base_domain5`)

   In general, whatever privileges were present for users in the first domain would continue to exist in new domain, provided user migration commands are used. To verify that the user migration commands were successful, make sure that user names are same in the first domain and the second domain.

5

Configuring Oracle Imaging and Process Management

This chapter describes how to configure an Oracle Imaging and Process Management (Oracle I/PM) application in an Oracle WebLogic Server domain.

This chapter includes the following sections:

- Section 5.1, "Completing the Oracle I/PM Configuration After First Login"
- Section 5.2, "Downloading Visual C++ Libraries for the Oracle I/PM Viewer (Windows System)"
- Section 5.3, "Configuring the Full-Text Features in the Oracle UCM Repository"
- Section 5.4, "Connecting to a BPEL Server"
- Section 5.5, "Resetting Oracle I/PM System Security"
- Section 5.6, "Installing and Configuring Oracle Application Extension Framework"
- Section 5.7, "Verifying the AXF Installation"
- Section 5.8, "Installing and Configuring Oracle Document Capture"

5.1 Completing the Oracle I/PM Configuration After First Login

The user who logs in first to an Oracle I/PM Managed Server is provisioned with full security throughout the server. When this user first logs in, Oracle I/PM provides a user interface to complete the configuration, including connecting to a repository or repositories and, optionally, to a Business Process Execution Language (BPEL) server.

> **Note:** In a production system, Oracle Enterprise Content Management Suite applications need to use an external Lightweight Directory Application Protocol (LDAP) authentication provider rather than the Oracle WebLogic Server embedded LDAP server, which is part of the default configuration. If you want to reassociate the identity store for Oracle I/PM with an external LDAP authentication provider, it is easier to do this before you complete the configuration of the Oracle I/PM Managed Server and before you connect it to the Oracle Universal Content Management (Oracle UCM) repository. For more information, see Section 4.4, "Reassociating the Identity Store with an External LDAP Authentication Provider."

To complete the Oracle I/PM configuration, you need to perform these tasks:

1. Adding the Agent User to Oracle WebLogic Server

2. Configuring Oracle Content Server 10g to work with Oracle I/PM

3. Adding the Administrator User and Administrators Group to Oracle UCM

4. Starting the Oracle I/PM Managed Server and Accessing the Web Client

5. Connecting to an Oracle UCM Repository

6. Configuring the AgentUser and GDFontPath MBeans

5.1.1 Adding the Agent User to Oracle WebLogic Server

To log in to Oracle WebLogic Server, Oracle I/PM services use the agent user, which is `agentadmin` by default. If you are using the Oracle WebLogic Server embedded LDAP server, you need to add this agent user, or a unique user name for the agent user, so the services can log in.

If you are using an external LDAP authentication provider, follow the steps for your identity store. For more information about external LDAP authentication providers, see Section 4.4, "Reassociating the Identity Store with an External LDAP Authentication Provider."

To add the agent user to Oracle WebLogic Server:

1. Start the Administration Server (see Section 7.1, "Starting the Administration Server").

2. Access the Oracle WebLogic Server Administration Console at

   ```
   http://adminServerHost:adminServerPort/console
   ```

   For `adminServerHost`, specify the name of the computer that hosts the Administration Server for your domain. For `adminServerPort`, specify the listen port number for the Administration Server. The default number is `7001`. For example:

   ```
   http://myHost:7001/console
   ```

   To log in, supply the user name and password that were specified on the Configure Administrator User Name and Password screen in the configuration wizard.

3. Click **Security Realms** (on the left).

4. In the Realms table on the Summary of Security Realms page, click **myrealm** in the **Name** column to open the Settings for myrealm page.

5. Go to **Users and Groups**, click **New**, and add the `agentadmin` user (or a unique user name).

5.1.2 Configuring Oracle Content Server 10g to work with Oracle I/PM

You need to configure Oracle Content Server before it can work with Oracle I/PM.

To configure Oracle Content Server 10g to work with Oracle I/PM:

1. Update the IP address filter:

   a. On the system where Oracle UCM is installed, navigate to the installation directory.

   b. Execute the `SystemProperties` application: `./bin/SystemProperties`

   c. Click the **Server** tab.

   d. In the **IP Address Filter** field, add a vertical bar (|) followed by the IP address of the system where Oracle I/PM is installed.

   The IP address is required for the Oracle I/PM system to have access to the Oracle UCM system without authentication.

   e. Click **OK**.

   This change will require a restart of Oracle Content Server, which you can do at the end of this procedure, after installing the Oracle UCM components.

2. Open the Oracle UCM Web client in a Web browser (`http://hostname:port/location`, such as `http://myhost.mycompany.com:8000/idc`), and log in.

3. Open the **Administration** tray.

4. Upgrade the default file store:

   a. Under **Administration**, select **Providers**.

   b. Select **Info** in the **Action** column of the **DefaultFileStore** row.

   c. When asked if you want to upgrade the file store, click **Upgrade**, and then click **Update** in the Edit File Store Provider dialog box.

   Oracle UCM does the upgrade automatically.

   Oracle I/PM content is not accessible in a Web store. Oracle Content Server traditionally uses a `weblayout` directory on a file system to store content in a format for viewing in a Web browser, but this feature does not have much use in an Oracle I/PM solution and uses extra disk space. After the file store upgrade, you should disable the `weblayout` functionality in Oracle Content Server for any file store provider configured for use as an Oracle I/PM volume.

5. Configure system properties:

   a. Confirm that the `SearchIndexerEngineName` variable matches the type of Oracle UCM system to use (`DATABASE.METADATA`, `DATABASE.FULLTEXT`, or `OracleTextSearch`).

   b. Under **Administration** tray, select **Admin Server**.

   c. Click **idc**.

   d. Select **General Configuration**, on the left.

   e. Select **Automatically assign a content ID on check in**.

   f. Specify an **Auto Number Prefix** value, such as **ucm1**.

     g. Set the `EnableIdcProfileField` variable to `1`:

       `EnableIdcProfileField=1`

     h. Click **Save**.

6. Install Oracle UCM components:

     a. Select **Component Manager**, on the left.

     b. In the Install New Component section, click **Browse**, and select any components in the Update Bundle `/component/CS10gR35UpdateBundle/extras` directory.

     c. Click **Open**.

     d. Click **Install**.

     e. Fill in any necessary details for each component you selected, and then click **Continue**.

     f. Click **here** to return to the Component Manager.

     g. In the Install New Component section, click **Browse**.

     h. Browse to the *ECM_ORACLE_HOME*`/ipm/lib` directory, and select **IpmRepository.zip**.

     i. Click **Open**.

     j. Click **Install**.

     k. Click **Continue**.

     l. Click **here** to return to the Component Manager.

     m. In the Install New Component section, click **Browse**.

     n. On the Oracle Enterprise Content Management Suite media disk, select **CS10gR35UpdateBundle.zip**.

     o. Click **Open**.

     p. Click **Install**.

     q. Click **Continue**.

     r. Select any installed component in the Update Bundle `/component/CS10gR35UpdateBundle/extras` directory and **IpmRepository**.

     s. Click **Enable**.

     t. Fill in any necessary details for each component you selected, and then click **Continue**.

     u. Click **here** to return to the Component Manager.

     v. From the Options list on the left, select **Start/Stop Content Server**.

     w. Select **Restart**.

     x. Ensure that Oracle Content Server is running after you restart it.

5.1.3 Adding the Administrator User and Administrators Group to Oracle UCM

You need to add the administrator user to Oracle UCM and assign it to the Administrators group before this user can perform administration tasks on Oracle UCM.

To add the administrator user and Administrators group to Oracle UCM

1. In the Oracle UCM Web client, select **Admin Applets** under **Administration**.

2. Click **User Admin**.

3. On the **Security** tab, select **Permissions By Role**.

4. Select **Add New Role**.

5. In the **Role Name** field, enter `Administrators`.

6. Click **OK**.

7. Click **Close**.

8. Click **Add**.

9. For **Authorization Type: Local**, click **OK**.

10. Create the administrator user, and enter the password.

11. Click the **Roles** tab.

12. Click **Add Role**.

13. Select **Administrators**, and then click **OK**.

14. Click **OK**.

15. Close the User Admin applet.

5.1.4 Starting the Oracle I/PM Managed Server and Accessing the Web Client

After you complete the preceding configuration tasks, you can start the Oracle I/PM Managed Server and access its Web client.

For transformations to work on some platforms, the following environment variables must be set before you start the Managed Server:

- Environment variables for library paths

    - Solaris Sparc: `LD_LIBRARY_ PATH=/usr/local/packages/gcc-3.4.2/lib`

Note: For document conversions on a Solaris SPARC platform, Oracle I/PM requires the GNU Compiler Collection (GCC) package 3.4.2 or later in the `/usr/local/packages` directory.

Install this package on the Solaris operating system that will run Oracle I/PM. You can download GCC from the Sunfreeware Web site at

http://www.sunfreeware.com

You also need to set the LD_LIBRARY_PATH environment variable to `/usr/local/packages/gcc-3.4.2/lib` before starting the Oracle I/PM Managed Server. If you are using a later version of GCC, set that version instead of `3.4.2`.

- AIX: `LIBPATH=$DOMAIN_HOME/oracle/imaging/imaging-server`

- HPI: `LD_PRELOAD=/usr/lib/hpux64/libpthread.so.1` and `LD_LIBRARY_PATH=$DOMAIN_HOME/oracle/imaging/imaging-server`

- DISPLAY environment variable

  On UNIX platforms running XWindows, when redirecting the display to a system with suitable graphic capabilities, set DISPLAY to a valid X Server.

To start the Oracle I/PM Managed Server and access the Web client:

1. Go to the `bin` directory under your domain home directory.

2. Start the Oracle I/PM Managed Server (see Section 7.2, "Starting Managed Servers").

3. Enter the administrator user name and password.

4. Wait until the Oracle I/PM Managed Server is running.

5. Access the Web client at this URL: `http://hostname:16000/imaging`

   Log in with the administrator user name and password.

   > **Note:** This first user to connect to the Oracle I/PM system is registered as the Oracle I/PM administrator.

5.1.5 Connecting to an Oracle UCM Repository

Before Oracle I/PM can use the Oracle UCM repository, you need to configure a connection to Oracle Content Server. You can create a connection to it from Oracle I/PM.

1. Open a Web browser, and navigate to this Web site:
   `http://hostname:16000/imaging`

2. Log in with the administrator user name and password.

3. Navigate to the **Manage Connections** tray, and select **Create Content Server Connection** from the list.

4. Enter a name for the connection on the **Basic Information** page, and optionally a description, and then click **Next**.

5. Enter the following values on the Connection Settings page:

   - **Repository Proxy:** `fmwadmin`

   - **Primary:** `localHost`

   - **Port:** The IDC port of the Oracle UCM instance, `4444` by default

6. Click **Next**.

   If you get the "Content Server does not have a defined document profile field" message, go to **General Configuration**, add the variable `EnableIdcProfileField=1`, and then restart Oracle Content Server.

7. Enter a **Connection Security** value for the connection.

   Select which users and groups should have permission to access, modify, delete, or grant others access to this connection definition.

8. Click **Next**.

9. At the Summary screen, click **Submit**.

5.1.6 Configuring the AgentUser and GDFontPath MBeans

Three agents run outside of Oracle I/PM, so you need to log into the Oracle I/PM system using a standard user in the security store. Oracle I/PM assigns security to this user name, which you need to configure as the agent user, by setting the `AgentUser` MBean.

To set the font path on a UNIX operating system, you also need to configure the `GDFontpath` MBean.

You can configure these MBeans through the System MBean Browser in Fusion Middleware Control.

To configure the AgentUser and GDFontPath MBeans:

1. Access the Oracle I/PM domain in Oracle Enterprise Manager 11*g* Fusion Middleware Control at the following URL:

```
http://adminServerHost:adminServerPort/em
```

For `adminServerHost`, specify the name of the computer that hosts the Administration Server for your domain. For `adminServerPort`, specify the listen port number for the Administration Server. The default number is `7001`. For example:

```
http://myHost:7001/em
```

To log in, supply the user name and password that were specified on the Configure Administrator User Name and Password screen in the configuration wizard.

2. In the navigation tree on the left, expand **Application Deployments**, and then click **imaging (IPM_server1)**.

3. On the **Application Deployment** menu, select **System MBean Browser**.

4. In the navigation tree on the System MBean Browser page, under **Configuration MBeans**, close the **com.bea** folder.

5. Expand the **oracle.imaging** folder, under **Application Defined MBeans**.

6. Expand the **Server: IPM_server1** and **config** folders.

7. Click **config**.

8. Set the value of the **AgentUser** attribute to `agentadmin` (or to a unique user name), click **Apply**, and then click **Return**.

9. On a UNIX operating system, set the value of the **GDFontPath** attribute to the location of your TTF files; for example:

```
/usr/share/X11/fonts/TTF
```

Some standard font locations on different UNIX platforms follow:

■ Solaris SPARC: `/usr/openwin/lib/X11/fonts/TrueType`

> **Note:** For document conversions on a Solaris SPARC platform, Oracle I/PM requires the GNU Compiler Collection (GCC) package 3.4.2 or later in the `/usr/local/packages` directory.
>
> Install this package on the Solaris operating system that will run Oracle I/PM. You can download GCC from the Sunfreeware Web site at
>
> http://www.sunfreeware.com
>
> You also need to set the LD_LIBRARY_PATH environment variable to `/usr/local/packages/gcc-3.4.2/lib` before starting the Oracle I/PM Managed Server. If you are using a later version of GCC, set that version instead of `3.4.2`.

- AIX: `/usr/lpp/X11/lib/X11/fonts/TrueType`
- HPI: `/usr/lib/X11/fonts/TrueType`

For systems on which Oracle WebLogic Server includes a JDK, you can find some True Type Fonts (TTF) in the `JDK/jre/lib/fonts` directory.

10. Click **Apply**.

11. Restart the Oracle I/PM Managed Server.

5.2 Downloading Visual C++ Libraries for the Oracle I/PM Viewer (Windows System)

The Oracle I/PM advanced viewer uses OutsideIn Technology, which requires the Visual C++ libraries included in the Visual C++ Redistributable Package for a Windows operating system. Three versions of this package (x86, x64, and IA64) are available from the Microsoft Download Center at

http://www.microsoft.com/downloads

Search for and download the version of the package that corresponds to the version of your Windows operating system:

- `vcredist_x86.exe`
- `vcredist_x64.exe`
- `vcredist_IA64.exe`

The required version of each of these downloads is the [Microsoft Visual C++] 2005 SP1 Redistributable Package. The redistributable module that Outside In requires is `msvcr80.dll`.

5.3 Configuring the Full-Text Features in the Oracle UCM Repository

Oracle I/PM supports two types of Full-Text under Oracle UCM: DATABASE.FULLTEXT and OracleTextSearch. Oracle I/PM can use the full-text features if you configure full-text searching in the Oracle UCM repository first. For DATABASE.FULLTEXT systems, after the indexes are rebuilt, nothing needs to be done on the Oracle I/PM side. OracleTextSearch, however, requires that the index be rebuilt every time a new application is built with the `FullText` option.

5.4 Connecting to a BPEL Server

A connection to a BPEL server is used to connect to the server through the BPEL EJB API. The information will be used for communication though the T3 protocol (not through HTTP). Before Oracle I/PM can connect to a BPEL server, you need to configure a connection to it. From the Oracle Imaging and Process Management user interface, you can create a BPEL connection and configure SSL for the BPEL server.

5.4.1 Creating a BPEL Connection

Before you can connect to the BPEL server, you need to create a BPEL connection from the Oracle I/PM Managed Server.

To create a BPEL connection:

1. Open a browser, and navigate to the following Web site:

   `http://`*`localHost`*`:7201/imaging`

2. Log in with the `weblogic` user name and password.

   > **Note:** This first user to connect to the Oracle I/PM system is registered as the administrator.

3. On the **Manage Connections** tab, select **Create BPEL Connection** from the list.

4. Enter a value in the **Name** field, in the format *`BPEL machine name`* `BPEL`, and, optionally, in the **Description** field.

   This parameter specifies the host name or names used for the connection. If the BPEL server is a single instance, it is the name or IP of the BPEL machine. If the BPEL server is operating within a cluster, this parameter value can be a comma-separated list of machine names or IP addresses of servers in the cluster, or it can be the name of the cluster.

   If multiple machine names are provided in a comma-separated list, the machines must *all* use the same port (the value supplied by the `port` parameter). If the BPEL Managed Servers in the cluster need to be defined with different ports, then the cluster-name configuration must be used.

   When a cluster name is used, the name must be defined in DNS to resolve to the multiple machines within the cluster. Neither Oracle I/PM nor BPEL defines this behavior. Rather, it is defined by the Oracle WebLogic Server support for JNDI in a cluster. For details on clustered JDNI support, see "Using WebLogic JNDI in a Clustered Environment" at the following Web site:

   `http://download.oracle.com/docs/cd/E12840_`
   `01/wls/docs103/jndi/jndi.html`

5. Click **Next**.

6. Enter the following value for **BPEL Machine name:** *`BPEL machine name`*`.us.oracle.com`

7. Enter the following value for **BPEL Port:** 8001

   This parameter specifies the port number used in the connection. For Oracle WebLogic Server, this is the standard listening port for the server. If the SSL option is selected, then the port provided must be the SSL listening port for the server, and T3 communication will actually use T3S, the SSL version of T3.

8. Select the SSL option if the target BPEL system requires it.

   This parameter indicates whether or not the port parameter is the SSL listening port of the BPEL server.

9. For **Credential Alias**, enter an alias previously created: `basic.credential`

   This parameter provides the alias of a user name and password that are stored in the Credential Store (CSF). These credentials are required to make the remote JNDI connection. The parameter is not the actual user name or password, but rather an alias (or key) used to look up the user name and password in the CSF, which encrypted them to provide for proper security.

   This credential must be created in the CSF before the BPEL connection configuration can be completed. A credential can be created in the CSF in one of two ways: through Fusion Middleware Control or through WebLogic Server Scripting Tool (WLST).

10. Click **Test Connection** to confirm the connection parameters to see what composites exist on that BPEL machine.

11. Click **Next**.

12. Optionally, alter security grants.

13. Click **Submit**.

5.4.2 Configuring SSL for the BPEL Server

For the Oracle I/PM SSL configuration to work with BPEL, the SSL listening port must be enabled on the BPEL server. This can be done at the time the BPEL server is first installed, through the configuration wizard, or after installation, through the Administration Console.

To configure SSL for the BPEL server:

1. Log in to the Administration Console for the BPEL Managed Server domain.

2. From Domain Structure, click **Environment** and then **Servers**.

3. Select the BPEL Managed Server instance.

4. Select **SSL Listen Port Enabled**.

5. Enter an available port number for **SSL Listen Port**.

6. Click **SAVE**.

   SSL is enabled on the BPEL Managed Server.

In the Oracle I/PM connection, the SSL option can be selected, and the SSL listen port can be used for the port parameter. At this point, T3 communication with the server will work properly if both the BPEL Managed Server and the Oracle I/PM Managed Server are configured to use the default `DemoTrust` certificates. All Oracle WebLogic Server instances use the same `DemoTrust` self-signed certificates and, therefore, are configured to trust the others by default.

You can also configure SSL for the BPEL server in the Oracle I/PM user interface, using the **Managed Connections** section to create the BPEL connection.

5.5 Resetting Oracle I/PM System Security

On a new Oracle I/PM system, the first user to log in is automatically granted full permissions. Typically, this initial user associates other users or groups, after which his or her permissions are changed or revoked as needed.

If security provider changes are made after this initial user login to Oracle I/PM, follow the steps below to reset Oracle I/PM system security. For example, if you later change the security configuration to point to an Oracle Internet Directory provider or a Microsoft Active Directory provider, you must reset Oracle I/PM system security.

1. Manually create or migrate users and groups to the new external security provider, using utilities as needed.

    For more information, see Section 4.4, "Reassociating the Identity Store with an External LDAP Authentication Provider."

2. Run the `refreshIPMSecurity()` WLST MBean command.

    For more information, see *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

    > **Note:** During the refresh, users or groups for whom matching identifying information is not found are ignored. As security changes are made, invalid users or groups are removed from the Oracle I/PM database.

5.6 Installing and Configuring Oracle Application Extension Framework

Oracle Application Extension Framework (AXF) is automatically installed with Oracle I/PM. For information about configuring and using AXF and the AXF database tables, see *Oracle Fusion Middleware E-Business Suite Adapter for Oracle Enterprise Content Management Administrator's Guide*.

5.7 Verifying the AXF Installation

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

5.7.1 HelloWorld Solution

Follow these steps to enable the HelloWorld solution.

1. As the AXF database user, run the `insertHelloCommand.sql` script from the *MW_HOME*/drivers/HelloWorld/dbscripts directory.

2. Access the driver page of the AXF Web application using the following URL:

    http://host:port/axf-web/faces/Driver.jspx

3. Enter the following values:

    - Solution Namespace: `HelloWorld`
    - Command Namespace: `Hi`
    - User Name: `jcooper`

> **Note:** This user name is valid only if you are using the application server's built-in `jazn.xml` security

4. Click **Execute Command**.

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

5.7.2 HelloBpel Solution

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

To enable the HelloBpel solution:

1. Edit and run the HelloBPEL SQL script (*MW_HOME*Oracle_ ECM1/ipm/lib/imaging-axf-install-extras.zip/drivers/HelloBpel /dbscripts/insertHelloWorldBpelData.sql), replacing `localhost` with your Application Server host name and modifying all password entries as required for your environment.

2. With JDeveloper 11.1.1.0, open the `HelloWorldBPELProcess.jpr` BPEL project and deploy it to your BPEL server. Consult the JDeveloper documentation for assistance with this task.

3. Access the driver page of the AXF Web application using the following URL:

   http://host:port/axf-web/faces/Driver.jspx

4. In the AXF Command Driver screen, enter the following values:

   - Solution Namespace: `HelloBpel`

   - Command Namespace: `OPEN_TASKLIST`

   - User Name: `jcooper`

   > **Note:** This user name is valid only if you are using the application server's built-in `jazn.xml` security

5. Click **Execute Command**.

   A response should be displayed in the response screen.

6. Click **Execute Response**, and log in when prompted.

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

5.8 Installing and Configuring Oracle Document Capture

For information about installing and configuring Oracle Document Capture on a client workstation, see *Oracle Document Capture Installation and Configuration Guide*.

6

Configuring Oracle Information Rights Management

This chapter explains how to configure an Oracle Information Rights Management (Oracle IRM) application in an Oracle WebLogic Server domain.

This chapter includes the following sections:

- Section 6.1, "Performing Postinstallation Configuration"
- Section 6.2, "Accessing the Oracle IRM Management Console"
- Section 6.3, "Configuring SSL for Oracle IRM"
- Section 6.4, "Configuring the Policy and Credential Store"
- Section 6.5, "Configuring the Identity Store"

6.1 Performing Postinstallation Configuration

Before logging in to the Oracle IRM Management Console or using Oracle IRM Desktop, you need to complete the Oracle IRM configuration, as these topics describe:

- Setting the Server URL Configuration Parameter for Oracle IRM
- Configuring a Key Store for Oracle IRM
- Configuring One-Way SSL for a Development Environment

> **Note:** In a production system, Oracle Enterprise Content Management Suite applications need to use an external Lightweight Directory Application Protocol (LDAP) authentication provider rather than the Oracle WebLogic Server embedded LDAP server, which is part of the default configuration. If you want to reassociate the identity store for Oracle IRM with an external LDAP authentication provider, it is easier to do this before you complete the configuration of the Oracle IRM Managed Server and before you connect it to the Oracle Universal Content Management (Oracle UCM) repository. For more information, see Section 4.4, "Reassociating the Identity Store with an External LDAP Authentication Provider."

6.1.1 Setting the Server URL Configuration Parameter for Oracle IRM

You can set the Server URL configuration parameter to an Oracle IRM Managed Server on the General Settings page for Oracle IRM in Fusion Middleware Control.

> **Caution:** The Server URL value is embedded into every sealed document, and Oracle IRM Desktop uses this value to identify and connect to an Oracle IRM server to retrieve licenses. This setting must not be changed after any documents have been sealed using this server, or no one will be able to access the documents.

For a simple installation where the Managed Server is directly accessible to Oracle IRM Desktop, this value will be the URI of the Managed Server. For example:

```
https://managedServerHost:managedServerPort/irm_desktop
```

To set the Server URL configuration parameter:

1. Start Oracle Enterprise Manager 11*g* Fusion Middleware Control at the following Web site:

    ```
    http://adminServerHost:adminServerPort/em
    ```

    For `adminServerHost`, specify the name of the computer that hosts the Administration Server for your domain. For `adminServerPort`, specify the listen port number for the Administration Server. The default number is `7001`. For example:

    ```
    http://myHost:7001/em
    ```

    To log in, supply the user name and password that were specified on the Configure Administrator User Name and Password screen in the configuration wizard.

2. From the farm navigation tree in Application Server Control, expand **Content Management** and **Information Rights Management**, and then click **irm**.

3. From the **IRM** menu, select **Administration** and then **General Settings**.

    Fusion Middleware Control displays the General Settings page.

4. In the **Server URL** field, enter the URL to access the Oracle IRM Managed Server.

    For example:

    ```
    https://irm.example.com/irm_desktop
    ```

    On the General Settings page, you can also specify other settings for Oracle IRM.

5. Click **Apply**.

6.1.2 Configuring a Key Store for Oracle IRM

To configure a key store for Oracle IRM, you need to create the key store and set its location and passwords. Due to algorithm restrictions with certain Java Cryptographic Extension (JCE) security providers, a number of different cryptographic algorithms and types of key stores are supported.

6.1.2.1 Choosing a Cryptographic Algorithm, Key Size, and Key Store

You should choose the most appropriate cryptographic algorithm, key size, and key store for the target platform. For most platforms the Advanced Encryption Standard (AES) key wrapping algorithm should be used. Other platforms require an RSA key wrapping algorithm.

6.1.2.1.1 AES Algorithm With the AES algorithm, the size of the wrapping key can either 256 bits or 128 bits. To seal content using the AES 256 cryptographic schema, you should use a 256 bit wrapping key. To seal content using the AES 128 cryptographic schema, you can use a 128 bit or 256 bit wrapping key. The AES key wrap algorithm is typically faster than the RSA key wrap algorithm.

6.1.2.1.2 RSA Algorithm For installing Oracle IRM on an AIX platform, the only supported key wrapping algorithm with the IBMJCE security provider is RSA. With RSA you should use a 2048 bit key.

6.1.2.2 Creating a Key Store

The Oracle IRM Java EE application uses a cryptographic key to wrap (encrypt) and unwrap (decrypt) Oracle IRM key data stored in the database. This wrapping key must be generated before contexts can be created.

The suggested location for the key store is under the domain home, in the *MW_HOME*/user_projects/domains/*domain_name*/config/fmwconfig directory (UNIX system) or *MW_HOME*\user_projects\domains*domain_name*\config\fmwconfig (Windows system). Placing the key store in this location ensures that the key store file is backed up when the domain and corresponding credential store files are backed up.

To create a key store for Oracle IRM:

1. Run the following script to set the environment.

   On a UNIX operating system:

   ```
   MW_HOME/wlserver_10.3/server/bin/setWLSEnv.sh
   ```

   On a Windows operating system:

   ```
   MW_HOME\wlserver_10.3\server\bin\setWLSEnv.cmd
   ```

   For the Java and Oracle WebLogic Server tools to work, you should have the weblogic.jar file in the *MW_HOME*/wlserver_10.3/server/lib directory (UNIX system) or *MW_HOME*\wlserver_10.3\server\lib directory (Windows system).

2. Run the keytool utility to generate an Oracle IRM key store as follows.

   ■ For AES, enter the following keytool command (the key size can be either 128 or 256):

   ```
   keytool -genseckey -storetype JCEKS -alias oracle.irm.wrap
        -keyalg AES -keysize 256 -keystore irm.jceks
   ```

   When prompted by keytool, choose appropriate passwords for the key store and the generated key.

■ For RSA, enter the following `keytool` command:

```
keytool -genkeypair -alias oracle.irm.wrap
        -keyalg RSA -keysize 2048 -keystore irm.jks
```

When prompted for the certificate details, use the suggested default value, `unknown`. When prompted by `keytool`, choose appropriate passwords for the key store and the generated key.

3. Copy the `irm.jceks` or `irm.jks` file to the *MW_HOME*/user_ projects/domains/*domain_name*/config/fmwconfig directory (UNIX system) or *MW_HOME*\user_projects\domains*domain_ name*\config\fmwconfig directory (Windows system).

6.1.2.3 Setting the Key Store Location

You can set the key store location with either Fusion Middleware Control or WebLogic Scripting Tool (WLST) commands.

6.1.2.3.1 Setting the Key Store Location with Fusion Middleware Control You can set the key store location on the Oracle IRM General Settings page in Fusion Middleware Control.

To set the key store location with Fusion Middleware Control:

1. Start Fusion Middleware Control at the following URL:

```
http://adminServerHost:adminServerPort/em
```

For *adminServerHost*, specify the name of the computer that hosts the Administration Server for your domain. For *adminServerPort*, specify the listen port number for the Administration Server. The default number is `7001`. For example:

```
http://myHost:7001/em
```

To log in, supply the user name and password that were specified on the Configure Administrator User Name and Password screen in the configuration wizard.

2. From the farm navigation tree in Fusion Middleware Control, expand **Content Management** and **Information Rights Management**, and then click **irm**.

3. From the **IRM** menu, select **Administration** and then **General Settings**.

4. In the **Keystore** field on the General Settings page, enter one of the following key store paths.

   ■ Key store path for an AES key store

      – On a UNIX operating system:

         MW_HOME/user_projects/domains/*domain_name*/config/fmwconfig/irm.jceks

      – On a Windows operating system:

         MW_HOME\user_projects\domains*domain_name*\config\fmwconfig\irm.jceks

   ■ Key store path for an RSA key store

      – On a UNIX operating system:

         MW_HOME/user_projects/domains/*domain_name*/config/fmwconfig/irm.jks

– On a Windows operating system:

    MW_HOME\user_projects\domains*domain_name*\config\fmwconfig\irm.jks

5. For the key store type, enter one of the following values:

   ■ `JCEKS` for an AES key store

   ■ `JKS` for an RSA key store

   On the General Settings page, you can also specify other settings for Oracle IRM.

6. Click **Apply**.

6.1.2.3.2 Setting the Key Store Location with WLST Commands You can set the key store location with the `connect` and `setIRMKeyStore` WLST commands.

To set the key store location with WLST commands:

1. Enter the following commands.

   On a UNIX operating system:

   ```
   ECM_ORACLE_HOME/common/bin/wlst.sh
   connect('username','password','t3://adminServerHost:adminServerPort')
   setIRMKeyStore()
   ```

   On a Windows operating system:

   ```
   ECM_ORACLE_HOME\common\bin\wlst.cmd
   connect('username','password','t3://adminServerHost:adminServerPort')
   setIRMKeyStore()
   ```

   You will be prompted for the key store path and key store type.

2. For the key store path, enter one of the following values.

   ■ Key store path for an AES key store

     – On a UNIX operating system:

       MW_HOME/user_projects/domains/*domain_name*/config/fmwconfig/irm.jceks

     – On a Windows operating system:

       MW_HOME\user_projects\domains*domain_name*\config\fmwconfig\irm.jceks

   ■ Key store path for an RSA key store

     – On a UNIX operating system:

       MW_HOME/user_projects/domains/*domain_name*/config/fmwconfig/irm.jks

     – On a Windows operating system:

       MW_HOME\user_projects\domains*domain_name*\config\fmwconfig\irm.jks

3. For the key store type, enter one of the following values.

   ■ `JCEKS` for an AES key store

   ■ `JKS` for an RSA key store

6.1.2.4 Setting Passwords for the Key Store

You must set passwords for the Oracle IRM key store with WLST commands. When the key store is created, you will be prompted for a key store password and a password for the generated key. These passwords are required by the Oracle IRM server.

To set passwords for the key store:

- For an AES key store, enter the following WLST commands.

  On a UNIX operating system:

  ```
  ECM_ORACLE_HOME/common/bin/wlst.sh
  connect('username','password','t3://adminServerHost:adminServerPort')
  createCred("IRM","keystore:irm.jks","dummy","password")
  createCred("IRM","key:irm.jceks:oracle.irm.wrap","dummy","password")
  ```

  On a Windows operating system:

  ```
  ECM_ORACLE_HOME/common/bin/wlst.cmd
  connect('username','password','t3://adminServerHost:adminServerPort')
  createCred("IRM","keystore:irm.jceks","dummy","password")
  createCred("IRM","key:irm.jceks:oracle.irm.wrap","dummy","password")
  ```

- For an RSA key store, enter the following WLST commands.

  On a UNIX operating system:

  ```
  ECM_ORACLE_HOME/common/bin/wlst.sh
  connect('username','password','t3://adminServerHost:adminServerPort')
  createCred("IRM","keystore:irm.jks","dummy","password")
  createCred("IRM","key:irm.jks:oracle.irm.wrap","dummy","password")
  ```

  On a Windows operating system:

  ```
  ECM_ORACLE_HOME/common/bin/wlst.cmd
  connect('username','password','t3://adminServerHost:adminServerPort')
  createCred("IRM","keystore:irm.jks","dummy","password")
  createCred("IRM","key:irm.jks:oracle.irm.wrap","dummy","password")
  ```

In the `connect` command, substitute the correct values for `username` and `password`.

In the `createCred` command, substitute for `password` the password that was used for creating the key and keystore.

The `"dummy"` parameter passed to the `createCred` command is the user name parameter. The key store does not use a user name, so this value is ignored. This is why the value is set as `dummy`.

It is normal for the `creatCred` command to return the text `"Already in Domain Runtime Tree"`. This text does not signify an error.

6.1.3 Configuring One-Way SSL for a Development Environment

For a development environment, you also need to configure one-way SSL with a server-specific certificate. One-way SSL means that only the server certificate passes from the server to the client but not the other way around.

To configure one-way SSL for a development environment:

1. Run the following script to set the environment.

   On a UNIX operating system:

   ```
   MW_HOME/wlserver_10.3/server/bin/setWLSEnv.sh
   ```

   On a Windows operating system:

   ```
   MW_HOME\wlserver_10.3\server\bin\setWLSEnv.cmd
   ```

   For the Java and Oracle WebLogic Server tools to work, you should have the `weblogic.jar` file in the `MW_HOME/wlserver_10.3/server/lib` directory (UNIX system) or `MW_HOME\wlserver_10.3\server\lib` directory (Windows system).

2. Use the `CertGen` utility to create a server-specific, private key and certificate, as follows:

   ```
   java utils.CertGen -selfsigned
                      -certfile MyOwnSelfCA.cer
                      -keyfile MyOwnSelfKey.key
                      -keyfilepass mykeypass
                      -cn "hostname"
   ```

   For `hostname`, substitute the name of the machine where Oracle IRM is deployed. You should use the same name while accessing Oracle IRM Web services. For example, to generate the server certificate for a machine named `myhost.us.example.com`, the command would be as follows:

   ```
   java utils.CertGen -selfsigned
                      -certfile MyOwnSelfCA.cer
                      -keyfile MyOwnSelfKey.key
                      -keyfilepass mykeypass
                      -cn "myhost.us.example.com"
   ```

   This command will generate a server certificate for the machine `myhost.us.example.com`. Verify that the certificate has been issued to the machine name you specified.

   `CertGen` creates a unique and secret Private Key for Oracle IRM and a Self-Signed Root Certificate.

3. Run the `ImportPrivateKey` utility to package the Private Key and Self-Signed Root Certificate into a keystore, as follows:

   ```
   java utils.ImportPrivateKey
                      -keystore MyOwnIdentityStore.jks
                      -storepass identitypass
                      -keypass keypassword
                      -alias trustself
                      -certfile MyOwnSelfCA.cer.pem
                      -keyfile MyOwnSelfKey.key.pem
                      -keyfilepass mykeypass
   ```

4. Run the `keytool` utility to package the key and certificate into a separate keystore called the Trust Keystore, as follows:

   ```
   keytool -import -trustcacerts -alias trustself
           -keystore TrustMyOwnSelf.jks
           -file MyOwnSelfCA.cer.der -keyalg RSA
   ```

5. On the client machine, double-click the certificate file to open the Certificate window, and then click **Install Certificate** to start the Certificate Import Wizard.

6. Install the certificate under Trusted Root Certification Authorities in Internet Explorer.

    On every machine running Oracle IRM Desktop, in the Certificate Import Wizard, explicitly select a certificate store for **Trusted Root Certification Authorities**. The root certificate must be trusted on *all* client computers that will access the server.

7. Click **Next**, and then follow the instructions on the wizard screens.

8. Set Up a Custom Identity Keystore and Trust Store:

    a. Log in to the Oracle WebLogic Server Administration Console, at the following URL:

    ```
    http://adminServerHost:adminServerPort/console
    ```

    For `adminServerHost`, specify the name of the computer that hosts the Administration Server for your domain. For `adminServerPort`, specify the listen port number for the Administration Server. The default number is `7001`. For example:

    ```
    http://myHost:7001/console
    ```

    To log in, supply the user name and password that were specified on the Configure Administrator User Name and Password screen in the configuration wizard.

    b. Select **Environments** under your domain from Domain Structure.

    c. Select **Servers** from **Environment**.

    d. From **Summary of Servers**, select the server for which to enable SSL.

    e. Click the **KeyStores** tab on the Settings for *servername* page.

    f. In the **KeyStores** field, select **Custom Identity and Custom Trust**.

    g. Enter values in the other fields on the **KeyStores** tab.

    h. Save the changes.

    i. Click the **SSL** tab.

    j. In the **Identity and Trust Locations** field, select **Keystores**.

    k. Enter values in the other fields on the **SSL** tab.

    l. Save the changes.

6.2 Accessing the Oracle IRM Management Console

When the Oracle IRM Managed Server is running, the Oracle IRM application is deployed and ready to be accessed through the Oracle IRM Management Console:

```
https://managedServerHost:managedServerPort/irm_rights
```

6.3 Configuring SSL for Oracle IRM

Oracle IRM requires SSL to be enabled on the front-end application, whether it is Oracle HTTP Server (OHS) or a Managed Server running Oracle IRM as an application deployed to Oracle WebLogic Server. Communication between Oracle IRM Desktop and the Oracle IRM server application must be over SSL because sensitive information such as passwords are communicated. Other uses of SSL, such as between OHS and Managed Servers, the Administration Server, and the LDAP authentication provider are optional.

6.4 Configuring the Policy and Credential Store

Oracle IRM uses the Credential Store Framework of Oracle Platform Security Services (OPSS) to retrieve passwords for the Oracle IRM key store. There are no specific configuration steps for Oracle IRM if the credential and policy stores are reassociated with an external LDAP authentication provider, as described in Section 4.4, "Reassociating the Identity Store with an External LDAP Authentication Provider."

6.5 Configuring the Identity Store

Oracle IRM uses OPSS to obtain user and group details from the external LDAP authentication provider. For information about configuring the identity store, see Section 4.4, "Reassociating the Identity Store with an External LDAP Authentication Provider."

7

Verifying the Installation and Configuration

This chapter explains how to verify successful installation and complete the configuration of Oracle Enterprise Content Management Suite applications.

This chapter includes the following sections:

- Section 7.1, "Starting the Administration Server"
- Section 7.2, "Starting Managed Servers"
- Section 7.3, "Starting Node Manager"
- Section 7.4, "Verifying the Installation"

7.1 Starting the Administration Server

Before you can start a Managed Server for an application, you need to start the Administration Server for the Oracle WebLogic Server domain.

To start the Administration Server:

1. Run the `startWebLogic.sh` script (UNIX system) or `startWebLogic.cmd` script (Windows system) from the `bin` directory under the domain home directory.

   The default domain home directory is *MW_HOME*`/user_projects/domains/`*domain_name* (UNIX system) or *MW_HOME*`\user_projects\domains\`*domain_name* (Windows system). Your domain name and directory path were provided on the Specify Domain Name and Location in Fusion Middleware Configuration Wizard.

   Note: On a Linux operating system, the shell is going to stay open.
   ---

2. For a production system, supply the Oracle WebLogic Server user name and password.

   Supply the values that were specified on the Configure Administrator User Name and Password screen in the configuration wizard.

3. Access the Oracle WebLogic Server Administration Console at the following URL:

   `http://adminServerHost:`*adminServerPort*`/console`

   For *adminServerHost*, specify the name of the computer that hosts the Administration Server for your domain. For *adminServerPort*, specify the listen

port number for the Administration Server. The default number is `7001`. For example:

```
http://myHost:7001/console
```

To log in, supply the user name and password that were specified on the Configure Administrator User Name and Password screen in the configuration wizard.

7.2 Starting Managed Servers

You can start each Managed Server from the `bin` directory inside your domain home directory, which is `MW_HOME/user_projects/domains/domain_name` (UNIX system) or `MW_HOME\user_projects\domains\domain_name` (Windows system). This information was provided on the Specify Domain Name and Location screen in the configuration wizard.

Important:

- Before starting an Oracle I/PM Managed Server and logging in for the first time, see Section 5.1, "Completing the Oracle I/PM Configuration After First Login," and do not start the Managed Server until you have completed the tasks before Section 5.1.4, "Starting the Oracle I/PM Managed Server and Accessing the Web Client."

- Before logging in to the Oracle IRM Management Console for the first time or using Oracle IRM Desktop, see Section 6.1, "Performing Postinstallation Configuration."

To start a Managed Server:

1. Start the Administration Server (see Section 7.1, "Starting the Administration Server").

2. Run the `startManagedWebLogic.sh` script (UNIX system) or `startManagedWebLogic.cmd` script (Windows system) from the `bin` directory in the domain home directory.

   This command requires that you specify a server name, such as one of these:

   - `IPM_server1` (Oracle Imaging and Process Management)

   - `IRM_server1` (Oracle Information Rights Management)

   For example, the following UNIX command would start an Oracle I/PM Managed Server:

   ```
   MW_HOME/user_projects/domains/domain_name/bin/startManagedWebLogic.sh IPM_
   server1
   ```

   The following Windows command would start an Oracle IRM Managed Server:

   ```
   MW_HOME\user_projects\domains\domain_name\bin\startManagedWebLogic.cmd IRM_
   server1
   ```

If you selected production mode, you will be prompted for the Oracle WebLogic Server user name and password before the server starts. These were provided on the Configure Administrator User Name and Password screen in the configuration wizard.

The names of the Managed Servers are in the `startManagedWebLogic_readme.txt` file. To view the server names on a UNIX operating system, issue this command:

```
cat MW_HOME/user_projects/domains/domain_name/startManagedWebLogic_readme.txt
```

To view the server names on a Windows operating system, double-click this file:

```
MW_HOME\user_projects\domains\domain_name\startManagedWebLogic_readme.txt
```

For information about stopping and starting a Managed Server with Oracle Enterprise Manager 11*g* Fusion Middleware Control, see "Starting and Stopping Oracle WebLogic Server Instances" in *Oracle Fusion Middleware Administrator's Guide*.

After you start a Managed Server the first time, you can create a `boot.properties` file in the *domain-home*/`servers`/*server-name*/`security/` directory. This filed would include the following lines:

```
username=USERNAME
password=PASSWORD
```

7.3 Starting Node Manager

Starting Node Manager on a machine that hosts one or more Managed Servers enables you to start and stop the Managed Servers remotely using the Administration Console or the command line. Node Manager can also automatically restart a Managed Server after an unexpected failure.

To start Node Manager:

1. Set the Node Manager properties with a script.

   On a UNIX operating system, run this script:

   ```
   ECM_ORACLE_HOME/common/bin/setNMProps.sh
   ```

   On a Windows operating system, run this script:

   ```
   ECM_ORACLE_HOME\common\bin\setNMProps.cmd
   ```

2. Start Node Manager with a script.

   On a UNIX operating system, run this script:

   ```
   WL_HOME/server/bin/startNodeManager.sh
   ```

   On a Windows operating system, run this script:

   ```
   WL_HOME\server\bin\startNodeManager.cmd
   ```

For more information about Node Manager, see *Oracle Fusion Middleware Node Manager Administrator's Guide for Oracle WebLogic Server*.

7.4 Verifying the Installation

To verify the installation of Oracle Enterprise Content Management Suite, start a Web browser, and enter the following URLs to test access to the WebLogic Administration Server, Administration Console, and Fusion Middleware Control, as well as to applications in your Oracle WebLogic Server domain.

- To access the Administration Server:

  ```
  http://adminServerHost:adminServerPort
  ```

  For `adminServerHost`, specify the name of the computer that hosts the Administration Server for your domain. For `adminServerPort`, specify the listen port number for the Administration Server. The default number is `7001`. For example:

  ```
  http://myHost:7001
  ```

  To log in, supply the user name and password that were specified on the Configure Administrator User Name and Password screen in the configuration wizard.

- To access the Administration Console:

  ```
  http://adminServerHost:adminServerPort/console
  ```

  For `adminServerHost`, specify the name of the computer that hosts the Administration Server for your domain. For `adminServerPort`, specify the listen port number for the Administration Server. The default number is `7001`. For example:

  ```
  http://myHost:7001/console
  ```

  To log in, supply the user name and password that were specified on the Configure Administrator User Name and Password screen in the configuration wizard.

- To access Fusion Middleware Control:

  ```
  http://adminServerHost:adminServerPort/em
  ```

  For `adminServerHost`, specify the name of the computer that hosts the Administration Server for your domain. For `adminServerPort`, specify the listen port number for the Administration Server. The default number is `7001`. For example:

  ```
  http://myHost:7001/em
  ```

  To log in, supply the user name and password that were specified on the Configure Administrator User Name and Password screen in the configuration wizard.

  In Fusion Middleware Control, you can configure the pages for Oracle Enterprise Management Suite applications.

- To test a newly set up Oracle I/PM instance:

  ```
  http://managedServerHost:managedServerPort/imaging
  ```

  Log in with the user name and password for Oracle WebLogic Server. The default port number for Oracle I/PM is `16000`.

- To test a newly set up Oracle IRM instance:

  ```
  https://managedServerHost:managedServerPort/irm_rights
  ```

  Log in with the user name and password for Oracle WebLogic Server. The default port number for Oracle IRM with SSL enabled is `16101`.

8

Deinstalling Oracle Enterprise Content Management Suite

This chapter explains how to deinstall Oracle Enterprise Content Management Suite.

This chapter includes the following section:

- Section 8.1, "Introduction to Deinstalling Oracle Enterprise Content Management Suite"
- Section 8.2, "Stopping Oracle Fusion Middleware Server and Processes"
- Section 8.3, "Removing Oracle Enterprise Content Management Suite Schemas"
- Section 8.4, "Deinstalling Oracle Enterprise Content Management Suite"
- Section 8.5, "Removing the Oracle Home Directories"

8.1 Introduction to Deinstalling Oracle Enterprise Content Management Suite

Deinstalling Oracle Enterprise Content Management Suite from your system involves the following tasks:

- Stopping Oracle Fusion Middleware Server and Processes
- Removing Oracle Enterprise Content Management Suite Schemas
- Deinstalling Oracle Enterprise Content Management Suite
- Removing the Oracle Home Directories

Use the instructions provided in this chapter for removing the software. If you try to remove the software manually, you may experience problems when you try to reinstall the software again at a later time. Following the procedures in this section will ensure that the software is properly removed.

8.2 Stopping Oracle Fusion Middleware Server and Processes

Before deinstalling Oracle Fusion Middleware software components, you should stop all servers and processes.

1. Stop each Oracle WebLogic Server Managed Server.

   On a UNIX operating system:

   ```
   MW_HOME/user_projects/domains/domain_name/bin/stopManagedWebLogic.sh managed_
   server_name admin_url username password
   ```

For example:

```
MW_HOME/user_projects/domains/ecm_domain/bin/stopManagedWebLogic.sh IPM_server1
t3://managedserver_hostname:managedserver_port weblogic password
```

On a Windows operating system:

```
MW_HOME\user_projects\domains\domain_name\bin\stopManagedWebLogic.cmd managed_
server_name admin_url username password
```

2. Stop the WebLogic Administration Server.

   On a UNIX operating system:

   ```
   MW_HOME/user_projects/domains/domain_name/bin/stopWeblogic.sh username password
   ```

   On a Windows operating system:

   ```
   MW_HOME\user_projects\domains\domain_name\bin\stopWeblogic.cmd username
   password
   ```

For more information, see "Starting and Stopping Oracle Fusion Middleware" in *Oracle Fusion Middleware Administrator's Guide*.

8.3 Removing Oracle Enterprise Content Management Suite Schemas

Run the Repository Creation Utility (RCU) to drop one or more Oracle Enterprise Content Management Suite schemas from your database.

8.3.1 Starting Repository Creation Utility

Insert the Repository Creation Utility DVD, and start RCU from the `rcuHome/bin` directory (UNIX system) or from the `rcuHome\BIN` directory (Windows system).

On a UNIX operating system:

```
./rcu
```

On a Windows operating system:

```
rcu.bat
```

If you download the Repository Creation Utility ZIP file from OTN, you can also start RCU as the preceding text describes.

8.3.2 Dropping Schemas

Follow these instructions to drop one or more Oracle Enterprise Content Management Suite schemas:

1. Welcome screen

   Click **Next**.

2. Create Repository screen

   Select **Drop**, and click **Next**.

3. Database Connection Details screen

   Provide the credentials to connect to your database instance. These are the same credentials you provided on this screen when you created the Oracle Enterprise Content Management Suite schemas. For more information, see Section 2.2, "Creating Oracle Enterprise Content Management Suite Schemas."

   Click **Next**. The Checking Prerequisites screen appears.

   If you have any prerequisite errors, the Database Connection Details screen displays details about the errors. Fix any errors, and click **Next** again.

   After the checking is complete with no errors, click **OK** to dismiss the screen.

4. Select Components screen

   Select a schema prefix, and then select the name of each schema you want to drop from the repository.

   Click **Next**. The Checking Prerequisites screen appears.

   If you have any prerequisite errors, the Select Components screen displays details about the errors. Fix any errors, and click **Next** again.

   After the checking is complete with no errors, click **OK** to dismiss the screen.

5. Summary screen

   Click **Drop**. A DROP screen appears.

   If you have any drop errors, the Summary screen displays details about the errors. Fix them, and click **Next** again.

   > **Note:** If your database is running on a Windows operating system, ensure that previous sessions accessing the tablespace are closed before the drop. After the drop, you might need to manually delete the dbf files.

   After the schemas are dropped with no errors, click **OK** to dismiss the screen.

6. Completion Summary screen

   Click **Close**.

8.4 Deinstalling Oracle Enterprise Content Management Suite

The deinstaller attempts to remove the Oracle home from which it was started. Before you remove the Oracle home for Oracle Enterprise Content Management Suite, make sure that it is not in use by an existing domain and that you stop all running processes that use this Oracle home. After you remove the software, you will no longer be able to use your WebLogic domain.

This procedure does not remove any WebLogic domains that you have created. It removes only the software in the ECM Oracle home.

Follow the instructions in Table 8–1 to deinstall Oracle Enterprise Content Management Suite. The procedure after the table describes these steps in more detail.

> **Note:** The deinstaller will attempt to remove the Oracle home directory from which it was started. Before you choose to remove the Oracle home, make sure that it is not in use by an existing domain.

Table 8–1   Deinstallation Procedure

No.	Screen	Description and Action Required
1	None.	Go to the *ECM_ORACLE_HOME*/oui/bin directory and start the deinstaller.
		On a UNIX operating system:

		<pre>cd ORACLE_HOME/oui/bin
		./runInstaller -deinstall [-jreLoc *jre_location*]</pre>

		On a Windows operating system:

		<pre>cd *ORACLE_HOME*\oui\bin
		setup.exe -deinstall [-jreLoc *jre_location*]</pre>

2	Welcome	Click **Next** to continue.
3	Deinstall Oracle Home	Verify the Oracle home you are about to deinstall.
		Click **Deinstall** to continue.
4	Deinstallation Progress	This screen shows the progress and status of the deinstallation.
5	Deinstallation Complete	Click **Finish** to dismiss the screen.

To deinstall Oracle Enterprise Content Management Suite:

1. Start the deinstaller from the *ECM_ORACLE_HOME*/oui/bin directory (UNIX system) or *ECM_ORACLE_HOME*\oui\bin directory (Windows system).

    On a UNIX operating system:

    ```
    ./runInstaller -deinstall [-jreLoc jre_location]
    ```

    On a Window operating system:

    ```
    setup.exe -deinstall [-jreLoc jre_location]
    ```

    The value of *jre_location* must specify the absolute path to the Java Runtime Environment (JRE) on your system. A relative path will not work.

    On a Windows operating system, you can also start the deinstaller from the **Start** menu by selecting **Programs**, then **Oracle ECM 11g - Home1**, and then **Uninstall**.

2. Welcome screen

    Click **Next**.

3. Deinstall Oracle Home screen

    Verify the ECM Oracle home you are about to deinstall, and click **Deinstall** to continue.

4. Deinstallation Progress screen

    No action is necessary on this screen, which shows the progress and status of the deinstallation.

5. Deinstallation Complete screen

    Click **Finish**.

8.5 Removing the Oracle Home Directories

Manually remove the ECM Oracle home directory and all of its subdirectories. For example, to remove the ECM Oracle home directory *MW_HOME*/`Oracle_ECM1` from a UNIX operating system:

```
cd /MW_HOME
rm -rf Oracle_ECM1
```

To remove the ECM Oracle home directory from a Windows operating system, you can use a file manager window, navigate to the `C:\`*MW_HOME* directory, right-click the `Oracle_ECM1` folder, and then select **Delete**.

You can also manually remove the program groups from the `Start Menu\Programs` folder, if they exist. For example, you might remove the following program groups from `C:\Documents and Settings\All Users\Start Menu\Programs`:

- **Oracle WebLogic (BEAHOME 1)**
- **Oracle ECM 11g - Home1**

The folder and program group names on your Windows system might be different.

9

Migrating a Domain from Test to Production

This chapter explains how to migrate an Oracle WebLogic Server domain from test to production for Oracle Enterprise Content Management Suite applications.

This chapter includes the following sections:

- Section 9.1, "Introduction to Migrating a Domain from Test to Production"
- Section 9.2, "Backing Up and Recovering a Domain"
- Section 9.3, "Migrating an Oracle IRM Domain from Test to Production"

9.1 Introduction to Migrating a Domain from Test to Production

You can migrate an Oracle Enterprise Content Management Suite application from test to production by using the test Oracle WebLogic Server domain to which the application is deployed as a template to install and reconfigure the domain on the production system. Your test domain might be a test, pilot, or proof of concept (POC) domain configured as a development system.

You can migrate a domain to roll out a template of an Oracle Information Rights Management (Oracle IRM) development domain to separate production domains for different customers, deploy a pilot Oracle IRM service to customers, or migrate a domain from production to a staging environment for upgrade testing.

Before you can migrate a domain, you need to back it up, or pack it. Then you can restore, or unpack. the domain in a different environment.

> **Note:** Before packing and unpacking an Oracle IRM domain, you need to configure a key store. For more information, see Section 6.1.2, "Configuring a Key Store for Oracle IRM."

9.2 Backing Up and Recovering a Domain

Some recommendations follow for backing up a domain that includes an Oracle Imaging and Process Management (Oracle I/PM) or Oracle IRM Managed Server.

9.2.1 Backup and Recovery Recommendations for Oracle IRM

The following Oracle Information Rights Management data must be backed up and restored.

- Configuration files, which are located in the domain home:

  MW_HOME/user_projects/domains/*domain_name* directory (UNIX system) or *MW_HOME*\user_projects\domains*domain_name* (Windows system)

- Database repository dependencies:

  ORAIRM schema

Backup Recommendations

Back up the domain, the ECM Oracle home, and the database containing the ORAIRM schema. Also, back up the LDAP directory and the key store.

> **Note:** The database and the key store must be kept synchronized. Back up both from the same point in time.

Recovery Recommendations

Restore the domain, the ECM Oracle home, and the shared file system, depending on the severity of the failure.

Recover the database containing the ORAIRM schema to the most recent point in time, if needed.

> **Note:** The database and the key store must be kept synchronized. If you restore one, restore the other to the same point in time.

9.2.2 Backup and Recovery Recommendations for Oracle I/PM

The following Oracle Imaging and Process Management data must be backed up and restored:

- Configuration files, which are located in the domain home:

  MW_HOME/user_projects/domains/*domain_name* directory (UNIX system) or *MW_HOME*\user_projects\domains*domain_name* (Windows system)

- Database repository dependencies:

  Oracle I/PM and Oracle UCM schemas.

Backup Recommendations

Back up the domain, the ECM Oracle home, and the database containing the schemas.

Recovery Recommendations

Restore the domain and the ECM Oracle home, depending on the severity of the failure.

Recover the database containing the schemas to the most recent point in time, if needed.

9.2.3 Backing Up Your Environment

For information about backing up an Oracle Enterprise Content Management Suite domain, see "Backing Up Your Environment" in *Oracle Fusion Middleware Administrator's Guide*.

9.2.4 Restoring an Oracle Enterprise Content Management Suite Domain

To restore an Oracle Enterprise Content Management Suite domain, you can recover the Oracle WebLogic Server domain, the database that includes your metadata repository, and the Oracle Information Rights Management and Oracle Imaging and Process Management applications.

9.2.4.1 Recovering an Oracle WebLogic Server Domain

You can recover an Oracle WebLogic Server domain that was corrupted or deleted from the file system.

> **Caution:** Performing a domain-level recovery can impact other aspects of a running system and all of the configuration changes performed after the backup was taken will be lost.

To recover an Oracle WebLogic Server domain:

1. Stop all relevant processes; that is, stop all processes that are related to the domain.

   For example, stop the Administration Server and Managed Servers. To stop the Administration Server, you can use the Oracle WebLogic Server Administration Console, WebLogic Scripting Tool (WLST), or the following script:

   ```
   DOMAIN_HOME/bin/stopWeblogic.sh username password admin_url
   ```

2. Recover the domain directory from backup:

   ```
   cd DOMAIN_HOME
   (UNIX) tar -xf domain_backup_092909.tar
   (Windows) jar xtf domain_backup_092909.jar
   ```

3. Start all relevant processes. That is, start all processes that are related to the domain. For example, start the Administration Server:

   ```
   DOMAIN_HOME/bin/startWebLogic.sh -Dweblogic.management.username=username
    -Dweblogic.management.password=password
    -Dweblogic.system.StoreBootIdentity=true
   ```

9.2.4.2 Recovering a Database

If your database that contains your metadata repository, including the MDS Repository, is corrupted, you can recover it using RMAN. You can recover the database at the desired level of granularity, either a full recovery or a tablespace recovery.

For best results, recover the database to the most current state, using point-in-time recovery (if the database is configured in Archive Log mode.) This ensures that the latest data is recovered. For example:

```
rman> restore database;
rman> recover database;
```

For detailed steps, see *Oracle Database Backup and Recovery User's Guide*, which is available on the Oracle Database Documentation page on Oracle Technology Network at

http://www.oracle.com/technology/documentation/database.html

9.2.4.3 Recovering Oracle Information Rights Management

To recover Oracle Information Rights Management:

1. Restore the domain, as described in Section 9.2.4.1, "Recovering an Oracle WebLogic Server Domain."

2. Restore the shared file system.

3. Restore the database, if necessary, as described in Section 9.2.4.2, "Recovering a Database."

> **Note:** The database and the key store must be kept synchronized. Back up both from the same point in time.

4. Restore the key store.

9.2.4.4 Recovering Oracle Imaging and Process Management

To recover Oracle Imaging and Process Management:

1. Restore the domain, as described in Section 9.2.4.1, "Recovering an Oracle WebLogic Server Domain."

2. Restore the database containing the Oracle I/PM and Oracle UCM schemas, if necessary, as described in Section 9.2.4.2, "Recovering a Database."

9.3 Migrating an Oracle IRM Domain from Test to Production

An Oracle WebLogic Server domain that includes an Oracle IRM Managed Server is an Oracle IRM domain. You can migrate Oracle IRM from a development test domain to a production domain. Oracle Fusion Middleware provides the following ways to migrate your Oracle IRM application:

- Rolling Out Templates of Oracle IRM Domains
- Deploying a Pilot Oracle IRM Service to Production
- Migrating a Production Environment to a Test Environment for Upgrades

9.3.1 Rolling Out Templates of Oracle IRM Domains

Organizations that host Oracle IRM as a service for customers, where each deployment needs to be completely separated from other deployments, can use templates of an Oracle IRM development domain to configure production domains for the customers. For example, Oracle On Demand might use this approach to rapidly deploy Oracle IRM applications for new customers.

The Oracle WebLogic Server domain that includes the Oracle IRM Managed Server in the source environment would be packed ready for deployment to the target environment. After the migration, the target environment would have a fully configured Oracle IRM Server, only requiring the server, host name, privacy policy URL, database, key store, and SSL certificate to be changed.

After unpacking a template Oracle IRM domain installation, you need to do the following configuration to make that installation machine specific and domain specific:

- Oracle WebLogic Server configuration

  A number of configuration settings are managed by Oracle WebLogic Server and are alterable using the Administration Console.

- Database Connection configuration

  Log in to the Administration Console using your administrator account, typically `weblogic`. Click **domain_name**, then **Services**, then **JDBC**, and then **Data Sources**. In the list there should be an entry for Oracle IRM. Click this entry. On the next page, click the **Connection Pool** tab. Depending on where the database is located and what the DBMS type is, the following settings might need to be changed:

  - Setting Description: Oracle SQL Server

    * URL, database host, and port details:
      `jdbc:oracle:thin:host:port/sid`
      `jdbc:sqlserver://host:port;database=database`

    * Driver Class Name: database specific, `oracle.jdbc.OracleDriver`
      `com.microsoft.sqlserver.jdbc.SQLServerDriver`

    * Properties: database user name

    * Password: database password

  - RCU

    This step is based on the assumption that the Oracle IRM schema has been installed on the database using Repository Creation Utility.

  - SSL

    For Oracle IRM, SSL should be enabled so that Oracle IRM Desktop does not show prompts to accept certificates when it contacts the Managed Server. The certificate used must be trusted by Microsoft Internet Explorer on computers running Oracle IRM Desktop.

    To set up SSL, follow the standard SSL setup instructions for Oracle WebLogic Server. You can find these instructions on the Configuring SSL page on Oracle Technology Network at

    `http://download.oracle.com/docs/cd/E15051_`
    `01/wls/docs103/secmanage/ssl.html`

- Oracle IRM Configuration

  A number of configurations for an Oracle IRM Managed Server are specific to an installation. These settings are stored in the JMX-managed configuration file `irm-config.xml`. The settings can be altered using Oracle Enterprise Manager 11*g* Fusion Middleware Control, WLST commands, or direct edits to the configuration file. Changing these settings with Fusion Middleware Control or WLST requires the Administration Server for the domain to be running.

  The Oracle IRM configuration file, `irm-config.xml` is in the *WL_ HOME*/config/fmwconfig directory.

■ Server URL

The Server URL setting is the URL value that is sealed into sealed content and used by Oracle IRM Desktop to request rights, keys, and settings. The value is typically the public-facing URL of the server pointing at the load balancer or Oracle HTTP Server (OHS). The default value is `https://irm.example.com/irm_desktop`.

This is a mandatory setting and must be specified.

You can use any of the following ways to set the Server URL:

– Fusion Middleware Control

The Server URL setting can be altered from the Oracle IRM General Settings page.

– WLST

The Server URL setting can be altered using the `setIRMServerURL` WLST command:

```
wls:/offline>
connect('weblogic','welcome1','t3://adminServerHost:adminServerPort')
wls:/base_domain/serverConfig>
setIRMServerURL('https://acme.example.com/irm_desktop')
```

For more information about the custom WLST commands for Oracle IRM, see *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

– Configuration file

The Server URL can be updated in the `classificationUrl` element of the configuration file:

```
<classificationUrl>https://irm.example.com/irm_desktop</classificationUrl>
```

■ Privacy URL

The Privacy URL setting is a URL to a page hosting the Oracle IRM usage privacy policy for the installation. There is no default value, so typically this setting will not need to be altered after unpacking a domain. The default behavior is to show the built-in privacy page.

You can set Privacy URL in any of the following ways:

– Fusion Middleware Control

The Privacy URL setting can be altered from the Oracle IRM General Settings page.

– WLST

The Privacy URL setting can be altered using the `setIRMPrivacyURL` command:

```
wls:/offline>
connect('weblogic','welcome1','t3://adminServerHost:adminServerPort')
wls:/base_domain/serverConfig>
setIRMPrivacyURL('http://acme.example.com/privacy')
```

For more information about the custom WLST commands for Oracle IRM, see *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

– Configuration file

The Privacy URL can be updated in the `privacyUrl` element:

```
<privacyUrl>http://acme.example.com/privacy</privacyUrl>
```
This is an optional setting. Absence of the `privacyUrl` element means that there is no privacy page configured.

■ Status Page Redirection

The Status Page Redirection setting is an optional URL to a page hosting alternative Oracle IRM Desktop status pages. There is no default value, so typically this setting will not need to be altered after a domain is unpacked. The default behavior is to use the built-in status pages.

You can set Status Page Redirection in any of the following ways:

– Fusion Middleware Control

The status page redirection settings can be altered from the Oracle IRM General settings page.

– WLST

The status page redirection settings can be altered using the setIRMStatusPageRedirectTarget command:

```
wls:/offline>
connect('weblogic','welcome1','t3://adminServerHost:adminServerPort')
wls:/base_domain/serverConfig>
setIRMStatusPageRedirectTarget('http://acme.example.com/status_pages',
'POST')
```

For more information about the custom WLST commands for Oracle IRM, see *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

– Configuration file

The Status Page Redirection setting can be updated in the `statusPageRedirectTarget` element:

```
<statusPageRedirectTarget>
    <uri>http://acme.example.com/status_pages</uri>
    <method>POST</method>
</statusPageRedirectTarget>
```

This is an optional setting. Absence of the `statusPageRedirectTarget` element means that there is no status page redirection configured.

■ Key store

Each Oracle IRM installation requires access to a key store with installation-specific keys. The unpacked domain may have a key store. If it does this key store must deleted and the passwords details cleared:

1. Delete the old key store.

   The key store file can be found in the `domain-home`/`config/fmwconfig` directory. This file is typically called `irm.jks`. Delete this file if it exists.

2. Clear the credentials.

   The key store passwords are stored in the credential store. If passwords have been set in the template domain; the passwords need to be cleared before you create a new key store. This is done using the following WLST commands:

   ```
   > connect('weblogic', 'welcome1', 'adminserver:')
   > deleteCred('IRM', 'keystore:irm.jks')
   > deleteCred('IRM', 'key:irm.jks:oracle.irm.wrap')
   ```

3. Create a new key store.

   The instructions used to create the key store after installation can be followed after unpacking a template domain. For more information, see Section 6.1.2, "Configuring a Key Store for Oracle IRM."

9.3.2 Deploying a Pilot Oracle IRM Service to Production

Organizations that run a proof of concept or pilot deployment can copy the operational service into a production environment.

In this scenario, you should ensure that the server host name used for the pilot is the host name that is required for the production service. The database and the entire Oracle WebLogic Server domain that includes the Oracle IRM Managed Server can then be backed up from the source (pilot) environment and deployed to the target (production) environment. All pilot content, contexts, and rights will be available after the migration.

A number of steps are required to move a pilot environment into a clustered production environment. The steps include backing up elements of the pilot installation, installing the production installation, and restoring pilot configuration and data.

Sealed Content

When moving from a pilot to production system, all sealed content created during the pilot installation can be used as long as the URL sealed into the content does not change.

Content URL

The domain name and protocol scheme used in the Oracle IRM server URL for the pilot must be the same as for the production system. Failure to do this will result in sealed content created during the pilot installation being unusable with the production system. It is therefore important to choose a domain name before starting the pilot installation; for example, choose something like `irm.example.com` rather than a machine-specific host name like `machine1234.example.com`. It is also important to ensure that SSL is used in the pilot system because switching from `http` in the pilot system to `https` in the production system would prevent pilot-sealed content from working in a production system.

After the pilot to production installation has been completed, the DNS entries for domain name can be switched from the pilot server to the production system.

Pilot System Backup

A number of elements of the pilot installation will be need to be manually backed up and used after the clustered production environment is installed:

- Database

  If the production database is different from the pilot database, you should make a backup of the Oracle IRM schema. This backup will be restored into the production database.

- Key store

  The Oracle IRM key store set up during the pilot installation should be backed up. This is typically called `irm.jks`. This file is usually located in the `domain-home`/config/fmwconfig directory. The key store and key passwords set during the pilot installation should also be recorded.

- Configuration

  The Oracle IRM configuration is stored in the JMX-managed configuration file `irm-config.xml`. This file can be in the `domain-home`/config/fmwconfig directory. You should make a copy of this file.

Production Installation

The production installation requires a full installation, apart from the Repository Creation Utility (RCU) database schema creation step.

RCU

The RCU schema installation should be skipped. This step should be replaced by a restore of the Oracle IRM schema from the database backup. If the pilot database is being used directly, there is no action to take.

Oracle WebLogic Server

Oracle WebLogic Server should be installed on the production system. Appropriate production-level settings should be selected.

Oracle Enterprise Content Management Suite

Oracle Enterprise Content Management Suite should be installed into the Middleware home for the Oracle WebLogic Server installation. During the configuration template stage, when database details are required, enter the database details of the backup. Appropriate cluster and production configuration settings should be made.

Manual Steps

After Oracle Enterprise Content Management Suite is installed, the pilot configuration and key store must be restored. This should be done before starting the Managed Servers. The Administration Server must be running.

Domain Home

The variable `domain-home` refers to the home directory of the Oracle WebLogic Server domain on which the Oracle IRM Java EE application is deployed. In examples, replace `domain-home` with the appropriate path.

Restoration of the Oracle IRM Configuration

The pilot configuration file, `irm-config.xml`, should be copied into the production `domain-home`/config/fmwconfig directory.

Oracle IRM Key Store Restoration

The pilot key store file (for example, `irm.jks`) should be copied into the production *domain-home*/`config/fmwconfig` directory.

Configuration Updates

The pilot configuration file may contain pilot specific settings, so the contents of this file should be reviewed. The following settings may require alteration:

- Privacy URL

  The Privacy URL setting is a URL to a page hosting the Oracle IRM usage privacy policy for the installation. There is no default value, so typically this setting will not need to be altered after unpacking a domain. The default behavior is to show the built-in privacy page.

  You can set Privacy URL in any of the following ways:

  - Fusion Middleware Control

    The Privacy URL setting can be altered from the Oracle IRM General Settings page.

  - WLST

    The Privacy URL setting can be altered using the `setIRMPrivacyURL` command:

    ```
    wls:/offline>
    connect('weblogic','welcome1','t3://adminServerHost:adminServerPort')
    wls:/base_domain/serverConfig>
    setIRMPrivacyURL('http://acme.example.com/privacy')
    ```

    For more information about the custom WLST commands for Oracle IRM, see *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

  - Configuration file

    The Privacy URL can be updated in the `privacyUrl` element:

    ```
    <privacyUrl>http://acme.example.com/privacy</privacyUrl>
    ```
    This is an optional setting. Absence of the `privacyUrl` element means that there is no privacy page configured.

- Status Page Redirection

  The Status Page Redirection setting is an optional URL to a page hosting alternative Oracle IRM Desktop status pages. There is no default value, so typically this setting will not need to be altered after a domain is unpacked. The default behavior is to use the built-in status pages.

  You can set Status Page Redirection in any of the following ways:

  - Fusion Middleware Control

    The status page redirection settings can be altered from the Oracle IRM General settings page.

- WLST

  The status page redirection settings can be altered using the setIRMStatusPageRedirectTarget command:

  ```
  wls:/offline>
  connect('weblogic','welcome1','t3://adminServerHost:adminServerPort')
  wls:/base_domain/serverConfig>
  setIRMStatusPageRedirectTarget('http://acme.example.com/status_pages',
  'POST')
  ```

  For more information about the custom WLST commands for Oracle IRM, see *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

- Configuration file

  The Status Page Redirection setting can be updated in the statusPageRedirectTarget element:

  ```
  <statusPageRedirectTarget>
      <uri>http://acme.example.com/status_pages</uri>
      <method>POST</method>
  </statusPageRedirectTarget>
  ```

  This is an optional setting. Absence of the statusPageRedirectTarget element means that there is no status page redirection configured.

■ Key store location

The key store location is stored in this configuration. The path should reflect the location of the restored pilot key store. The suggested location for the key store file is the *domain-home*/config/fmwconfig directory.

You can set the key store location in any of the following ways

- Fusion Middleware Control

  The key store path can be set on the Oracle IRM General settings page.

- WLST

  The key store location can be altered using the setIRMKeyStore command:

  ```
  wls:/offline>
  connect('weblogic','welcome1','t3://adminServerHost:adminServerPort')
  wls:/base_domain/serverConfig> setIRMKeyStore('JKS',
  '${domain.home}/config/fmwconfig/irm.jks')
  ```

- Configuration file

  The key store path and key store type can be updated in the keyStore element.

  ```
  <keyStore>
      <type>JKS</type>
      <path>${domain.home}/config/fmwconfig/irm.jks</path>
  </keyStore>
  ```

■ Key store passwords

The Oracle IRM Java EE application needs a password for the key store and each key stored in the key store. If the passwords are not specified, the Oracle IRM Java EE application will not be able to retrieve the keys. WLST commands can be used to set the credentials. The next example shows connecting to an Administration Server and setting the key store credentials.

In the following example, the key store is called `irm.jks`. Replace both occurrences of *password* with appropriate values for the production system.

```
> connect("weblogic", "welcome1", "t3://adminServerHost:adminServerPort")
> createCred("IRM", "keystore:irm.jks", "dummy", "password")
> createCred("IRM", "key:irm.jks:oracle.irm.wrap", "dummy", "password")
```

If the key store and key passwords are to be changed in a production system, use the `keytool` command-line application to change the passwords prior to setting the passwords using the WLST commands.

9.3.3 Migrating a Production Environment to a Test Environment for Upgrades

Organizations can test a server upgrade in a staging environment before upgrading the production server. They can also use the production-to-test procedure for testing an integration.

The database and the entire Oracle WebLogic Server domain that include the Oracle IRM Managed Server will be backed up from the source (production) environment and deployed to the target (test) environment. The host name (and SSL certificate) will be changed so that production content cannot be accessed via the test server. All production contexts and rights will be available after the migration; but new test content will be required for end-to-end testing.

A

Oracle Enterprise Content Management Suite Installation Screens

This appendix describes Oracle Fusion Middleware 11g ECM Suite Installation screens for installing the Oracle Enterprise Content Management Suite component of Oracle Fusion Middleware:

- Welcome
- Prerequisite Checks
- Specify Installation Location
- Installation Summary
- Installation Progress
- Installation Completed

A.1 Welcome
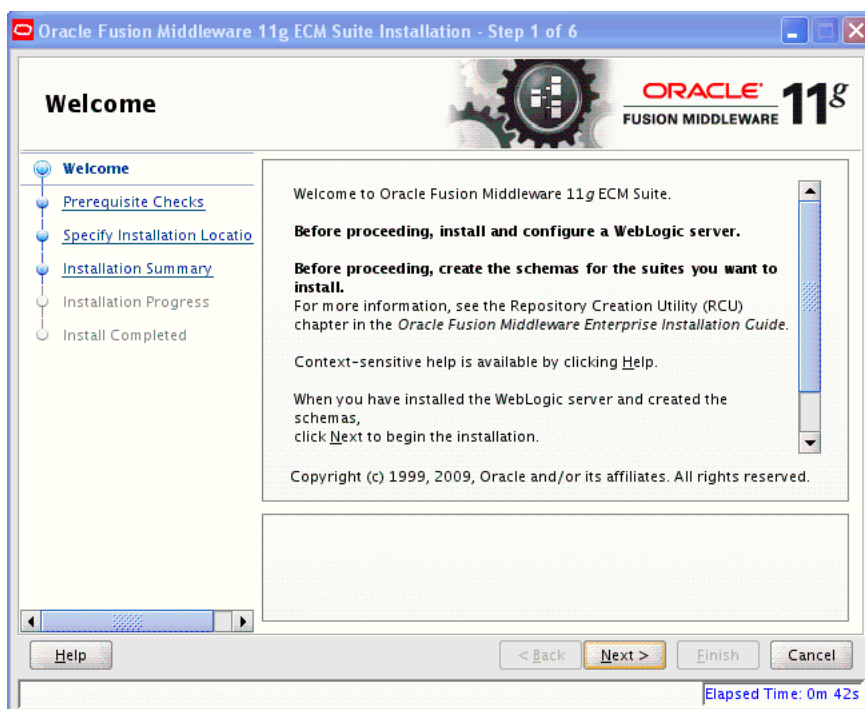
Each time the installer starts, it displays the Welcome screen.

The **Next** button continues the installation.

The **Cancel** button stops the installation.

A.2 Prerequisite Checks
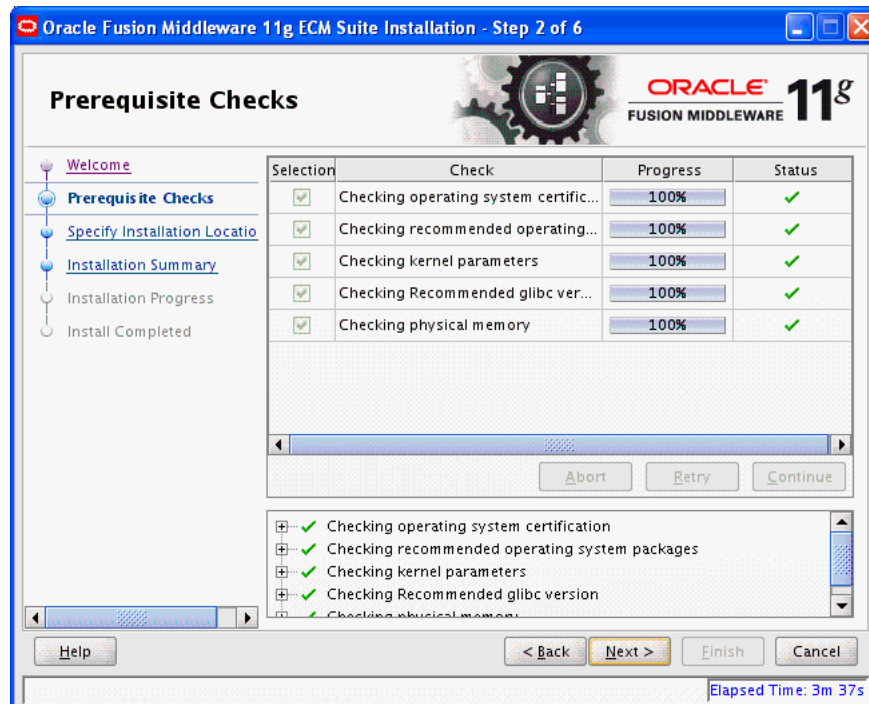
This screen shows the prerequisite checks for a UNIX operating system. Only three checks are performed for a Windows operating system:

■ Checking operating system certification

■ Checking Service Pack

■ Checking physical memory

The installer displays any error or warning messages in the bottom section of the screen.

The **Abort** button stops prerequisite checking for all applications.

The **Retry** button starts prerequisite checking again for all applications.

The **Continue** button continues the installation even if the screen displays an error or warning message.

The **Back** button returns to the Welcome screen.

The **Next** button continues the installation after the prerequisite check completes with no errors.

The **Cancel** button stops the installation.

A.3 Specify Installation Location
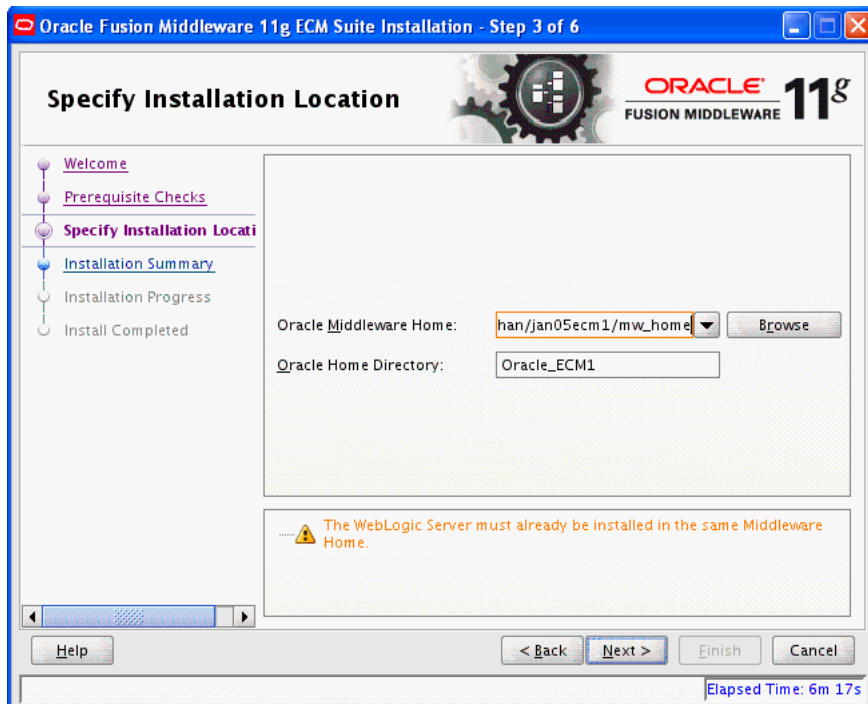
The **Oracle Middleware Home** field specifies the absolute path to an existing Middleware home directory. The **Browse** button displays directories that exist on your system.

The **Oracle Home Directory** field specifies a directory, inside the Middleware home directory, in which to install Oracle Enterprise Content Management Suite (the ECM Oracle home directory). This directory must be empty. If the directory does not exist, the installer creates it.

The ECM Oracle home directory is where all Oracle Enterprise Management Content Suite products will be installed. All software binaries will reside in this directory, and no runtime process can write to this directory.

The **Back** button returns to the previous screen.

The **Next** button continues the installation after the prerequisite check completes with no errors.

The **Cancel** button stops the installation.

A.4 Installation Summary
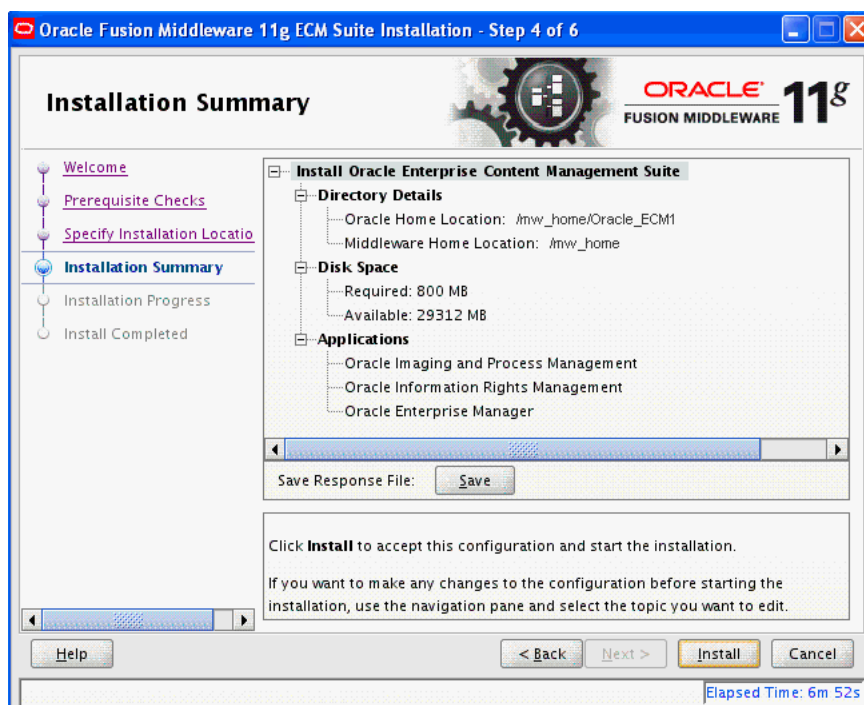
This screen summarizes the installation configuration.

The **Save** button saves the installation configuration in a file, which you can use later to perform the same installation from the command line.

The **Back** button or a link in the navigation tree on the left returns to a previous screen, where you can change the configuration.

The **Install** button begins the installation, with the configuration summarized on this screen.

The **Cancel** button stops the installation.

A.5 Installation Progress
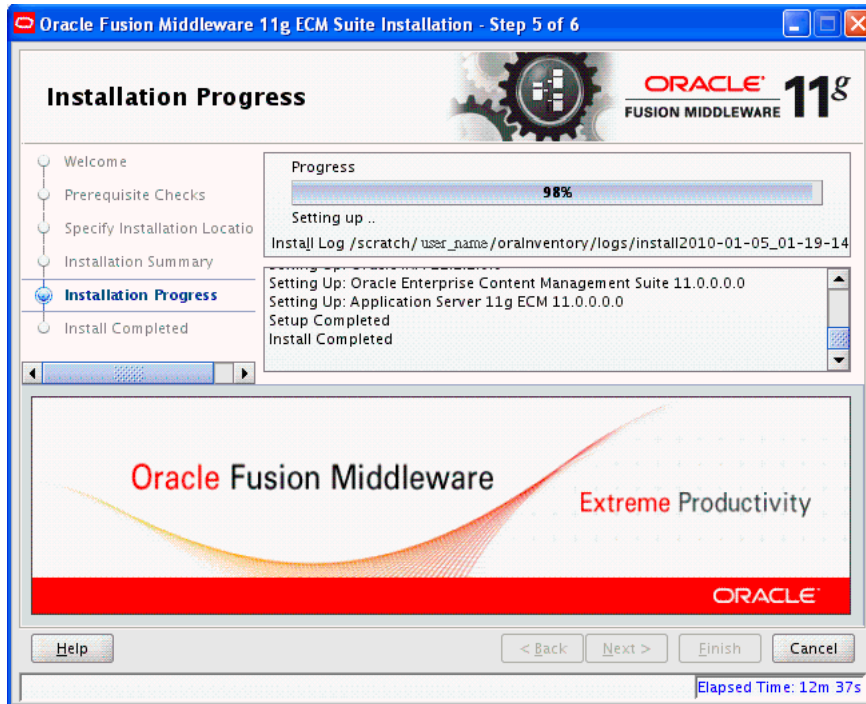
This screen shows you the percentage of progress for the installation.

The **Cancel** button stops the installation before it completes.

A.6 Installation Completed
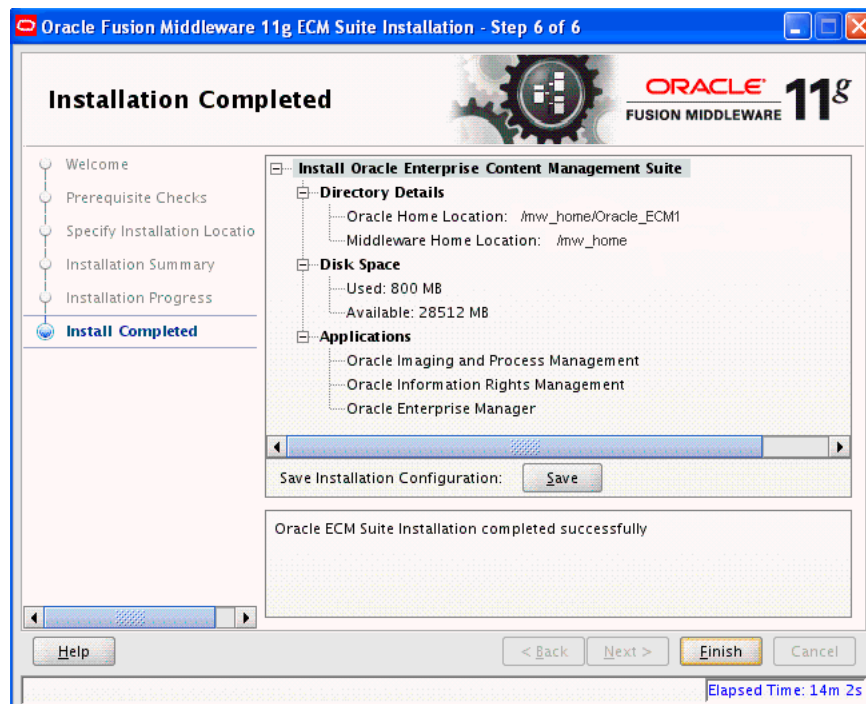
This screen indicates that the installation of Oracle Enterprise Content Management Suite is complete and summarizes its configuration.

The **Save** button saves the installation configuration in a file, which you can use later to perform the same installation from the command line.

The **Finish** button exits the configuration wizard.

B

Oracle Enterprise Content Management Suite Configuration Screens

This appendix describes the Fusion Middleware Configuration Wizard screens for configuring Oracle Enterprise Content Management Suite applications:

- Welcome
- Select a WebLogic Domain Directory
- Select Domain Source
- Select Extension Source
- Specify Domain Name and Location
- Configure Administrator User Name and Password
- Configure Server Start Mode and JDK
- Configure JDBC Component Schema
- Test Component Schema
- Select Optional Configuration
- Configure the Administration Server
- Configure Managed Servers
- Configure Clusters
- Configure Machines
- Target Deployments to Clusters or Servers
- Target Services to Clusters or Servers
- Configure RDBMS Security Store Database
- Configure Key Store Credentials
- Configuration Summary
- Creating Domain
- Creating Domain (Extended Domain)

B.1 Welcome
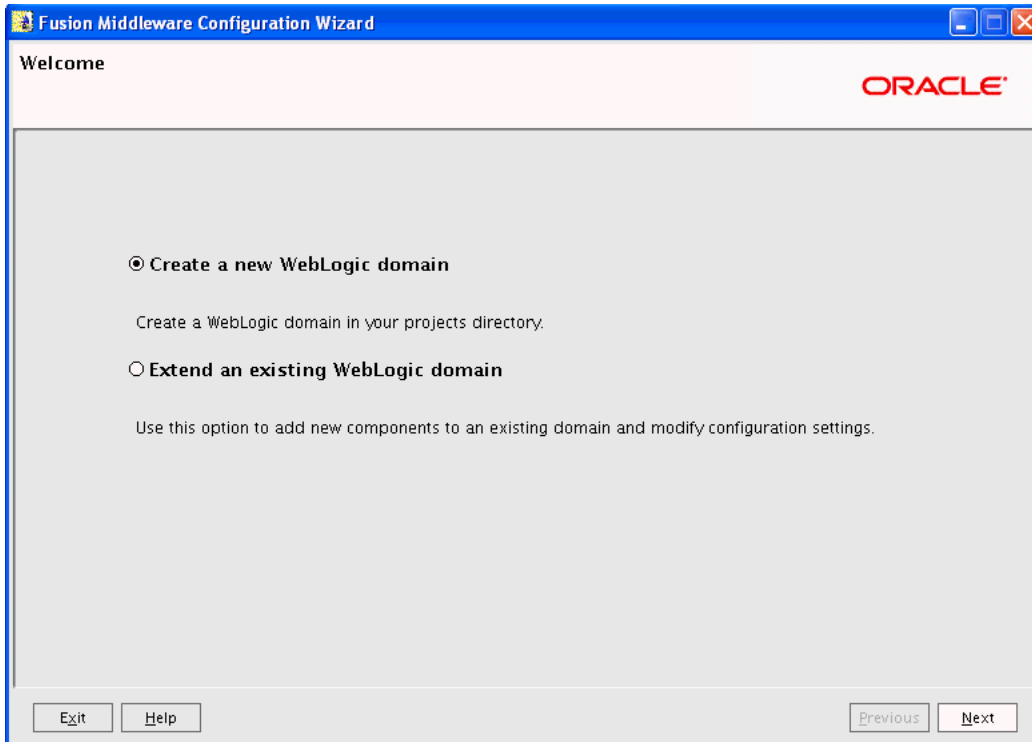
The Welcome screen appears each time you start the configuration wizard.

Select **Create a new WebLogic domain** to create a new WebLogic domain in your `projects` directory.

Select **Extend an existing WebLogic domain** if you want to add applications and services, or to override existing database access (JDBC) and messaging (JMS) settings.

Click **Next** to continue.

B.2 Select a WebLogic Domain Directory
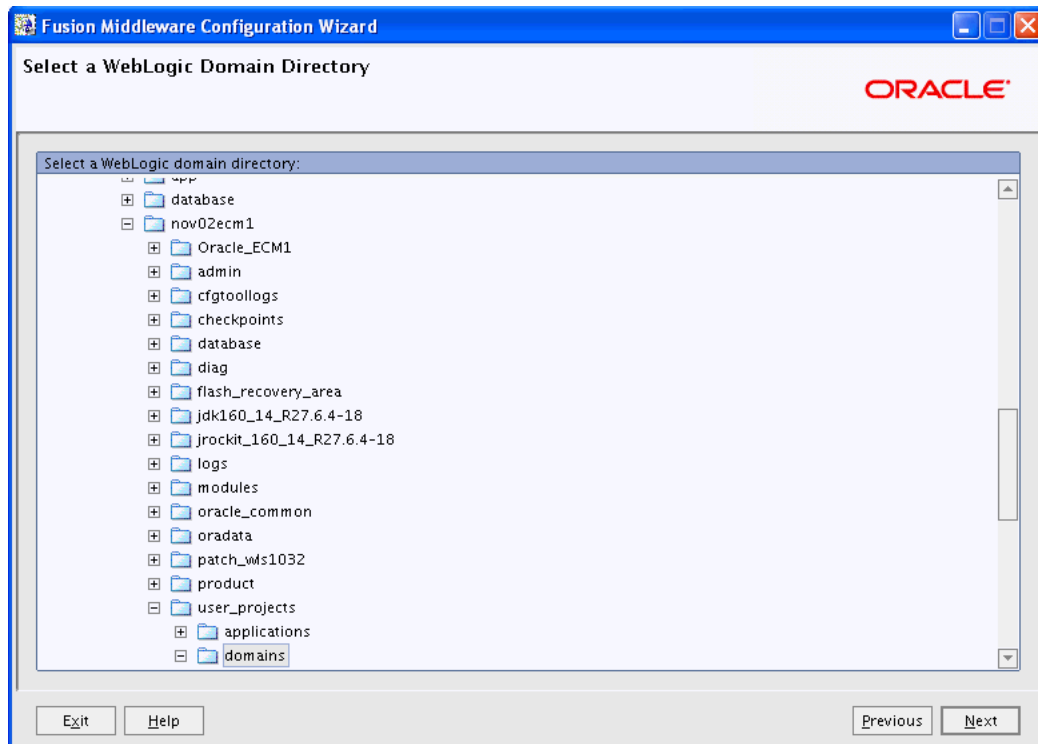
Select the WebLogic directory to which you want to add your applications or services, or both.

Click **Next** to continue.

B.3 Select Domain Source
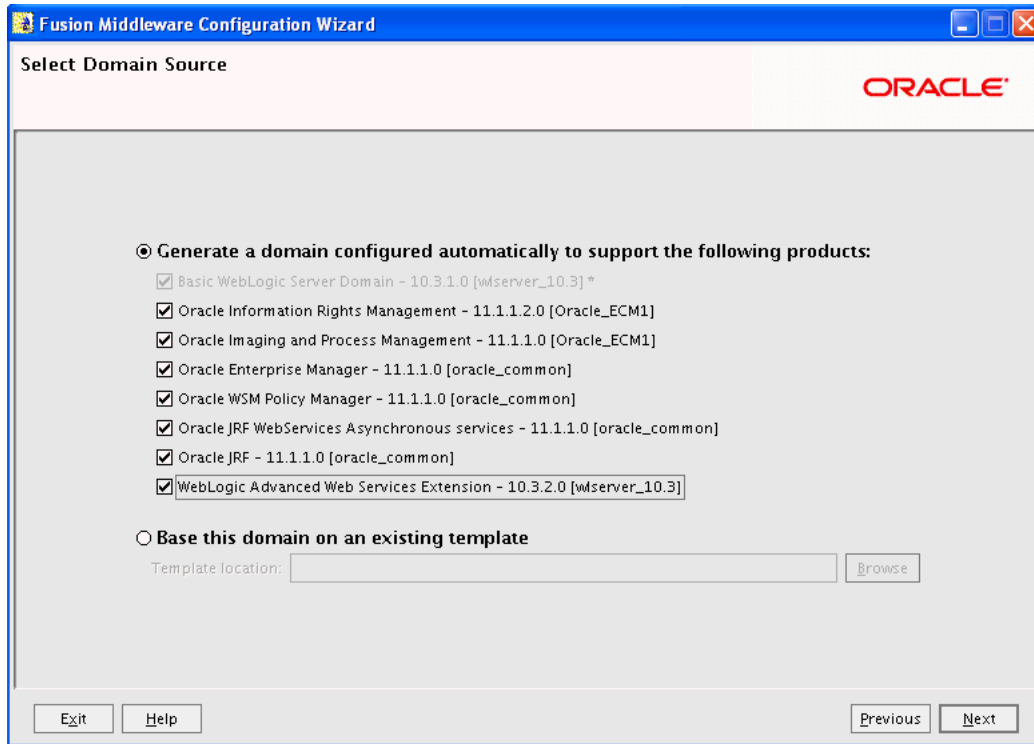
Select the source from which to create a new Oracle WebLogic Server domain. Select **Generate a domain automatically to support the following products**, and then select the products.

When you select **Oracle Imaging and Process Management** or **Oracle Information Rights Management** on the Select Domain Source screen, **Oracle Enterprise Manager** and **Oracle JRF** are automatically selected.

Select **Base this domain on an existing template** to create your domain based on an existing domain template. Click **Browse** to navigate your directories to find an existing template.

Click **Next** to continue.

B.4 Select Extension Source
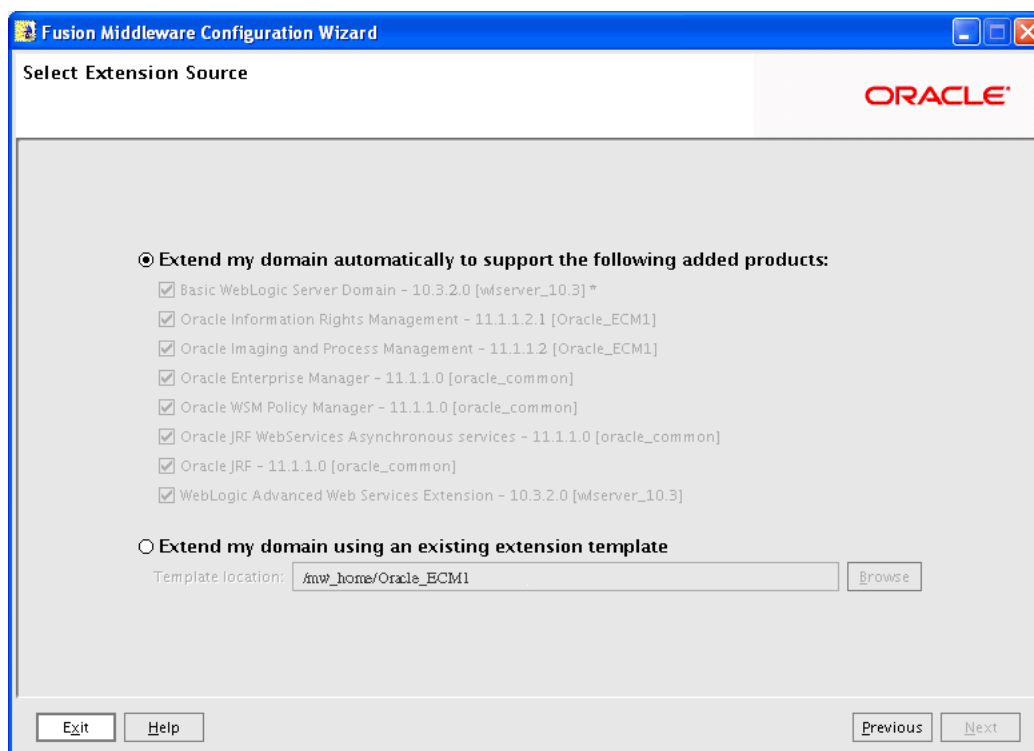
Select the source from which to extend an existing Oracle WebLogic Server domain. Select **Extend my domain automatically to support the following added products**, and then select the products.

When you select **Oracle Imaging and Process Management** or **Oracle Information Rights Management** on the Extend Domain Source screen, **Oracle Enterprise Manager** and **Oracle JRF** are automatically selected.

Select **Extend my domain using an existing extension template** to extend your domain based on an existing extension template. Click **Browse** to navigate your directories to find an existing template.

Click **Next** to continue.
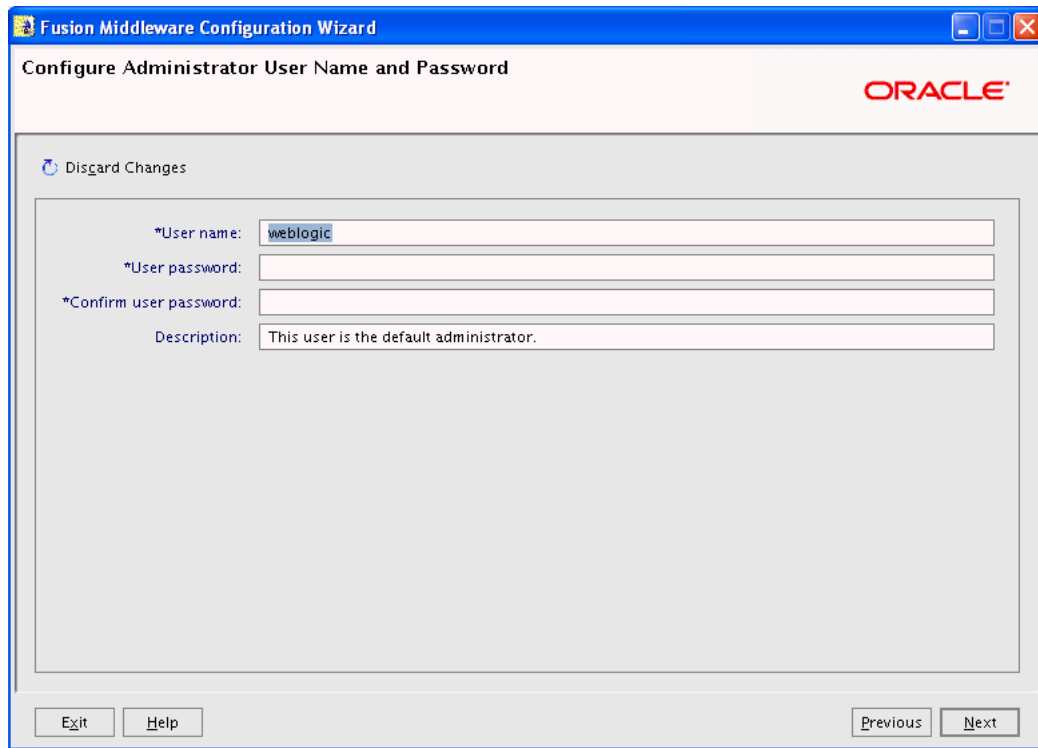
B.5 Specify Domain Name and Location
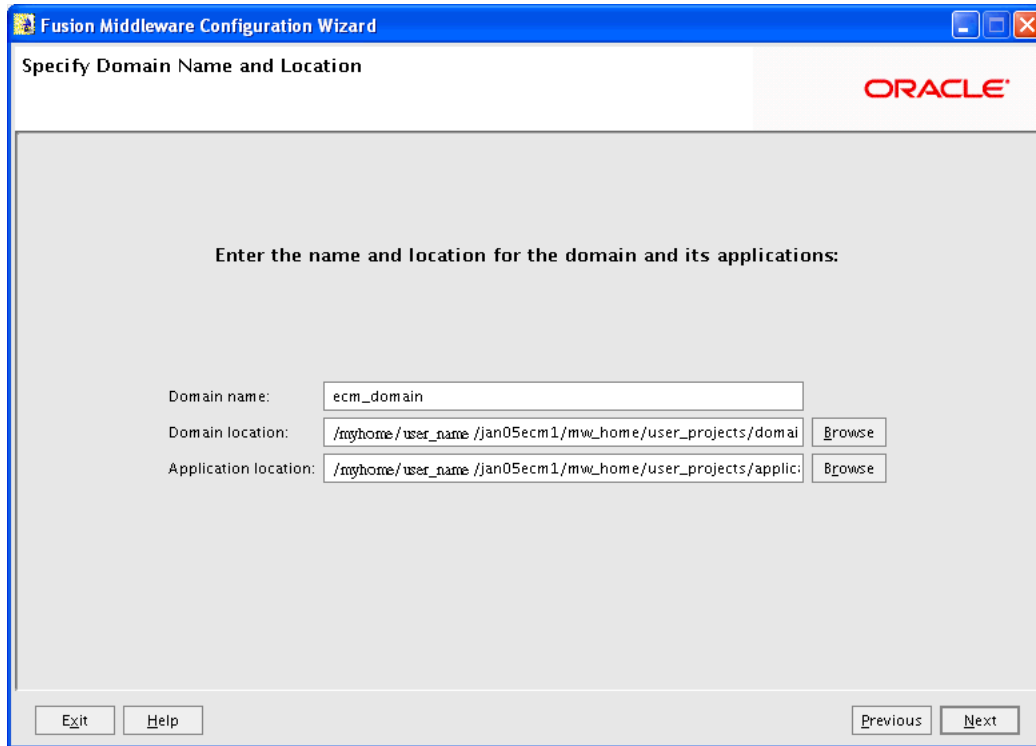
Use the default domain name, domain location, and application location, or specify different ones.

Click **Next** to continue.

B.6 Configure Administrator User Name and Password

Create a user that will be assigned to the Administrator role. This user is the default administrator for starting development mode servers.

- **User name**

  Specify the user name.

- **User password**

  Specify the password for the user.

- **Confirm user password**

  Reenter the user password.

- **Description**

  Enter a description for the user. This field is optional.

Click **Next** to continue.

B.7 Configure Server Start Mode and JDK
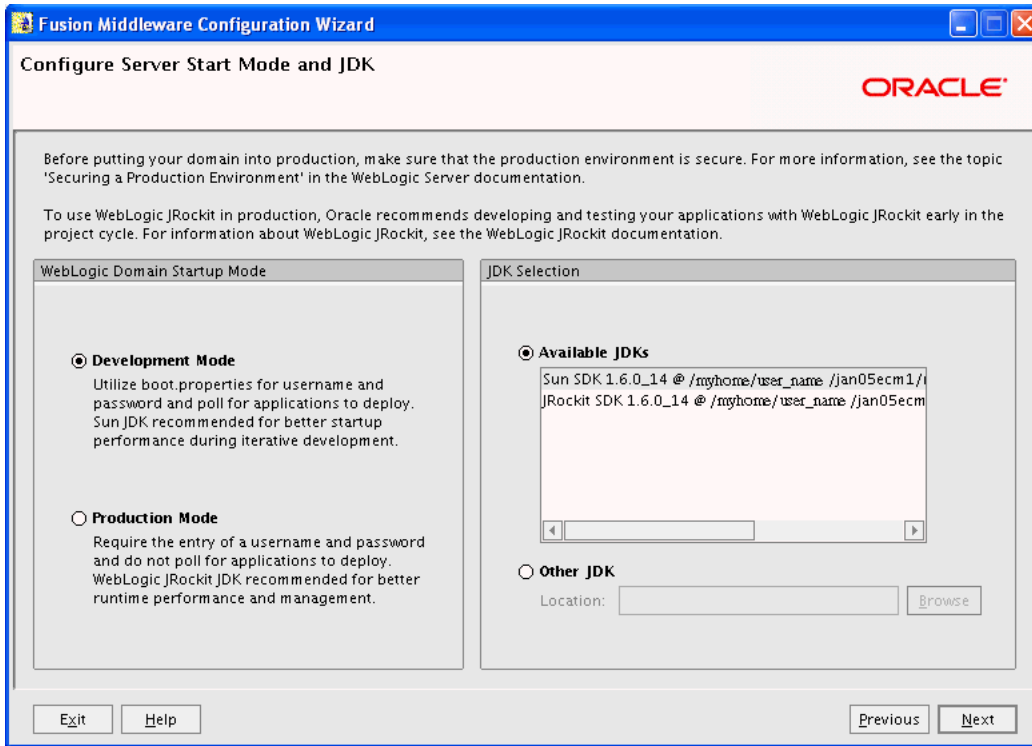
In the WebLogic Domain Startup Mode section, select one of the following startup modes:

- **Development Mode**

  In this mode, `boot.properties` is used for user names and passwords, and polling is used for application deployment. Sun SDK is the default for this mode.

- Production Mode

  In this mode, user names and passwords are required, and polling is not used for application deployment. JRockit SDK is the default for this mode.

In the JDK Selection section, select a JDK from the list of available JDKs, or select **Other JDK**, and then click **Browse** to find another JDK on your system.

Click **Next** to continue.

B.8 Configure JDBC Component Schema

Use this screen to edit the configuration information for each JDBC component schema.

A component schema contains a pool of database connections. Your application uses a component schema by looking it up in the JNDI tree, requesting a connection, using the connection, and then returning the connection to the component schema.

Click **Next** to continue.

B.9 Test Component Schema
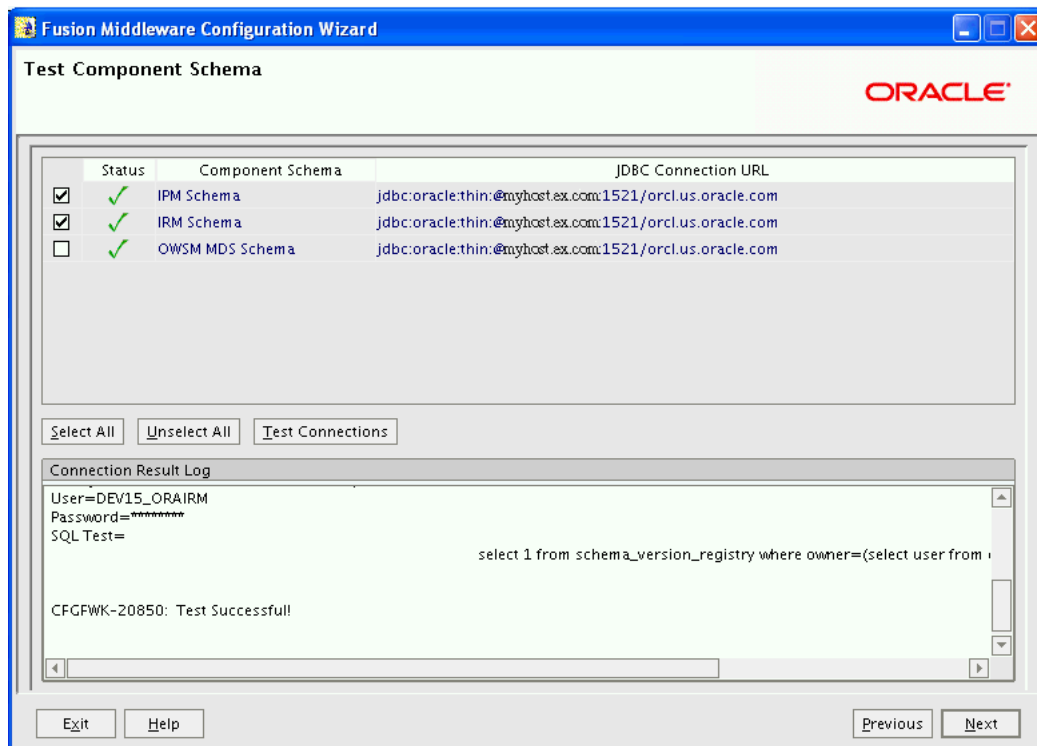
Use this screen to test JDBC connections to application schemas.

Click **Select All** to select all of the schemas for connection testing, or select one or more individual schemas.

Click **Unselect All** to deselect all of the schemas.

Click **Test Connections** to test the JDBC connections to the selected schema or schemas.

The Connection Result Log section shows the results of connection testing.

Click **Next** to continue.

B.10 Select Optional Configuration
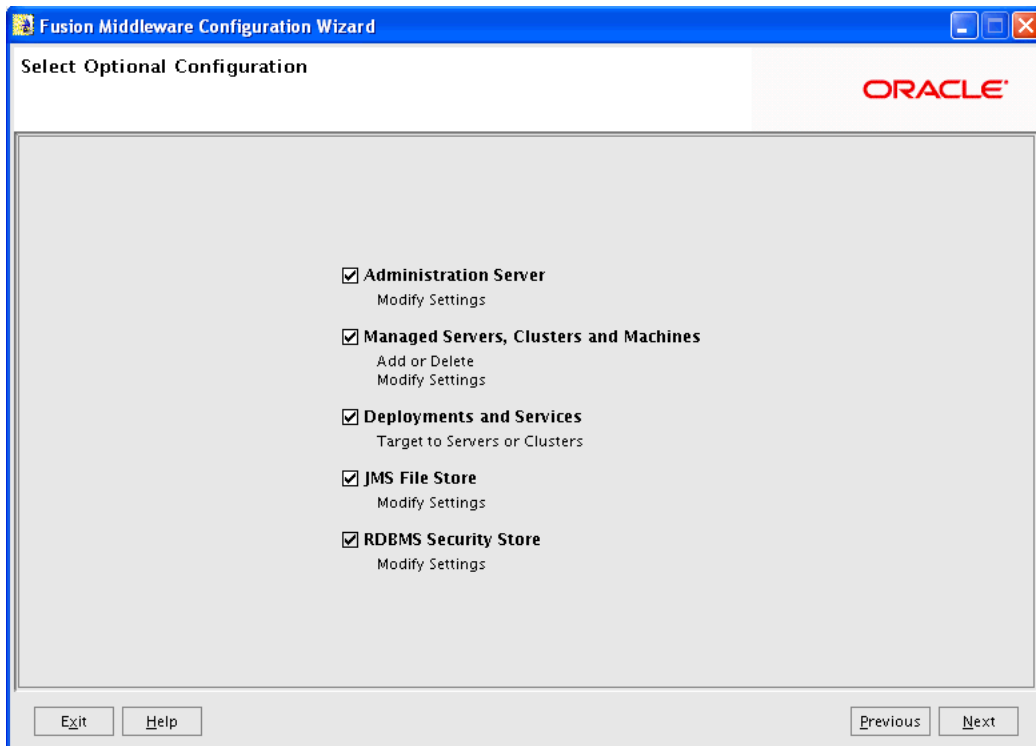
Select any of the server and cluster settings that you want to customize.

Click **Next** to continue.

B.11 Configure the Administration Server
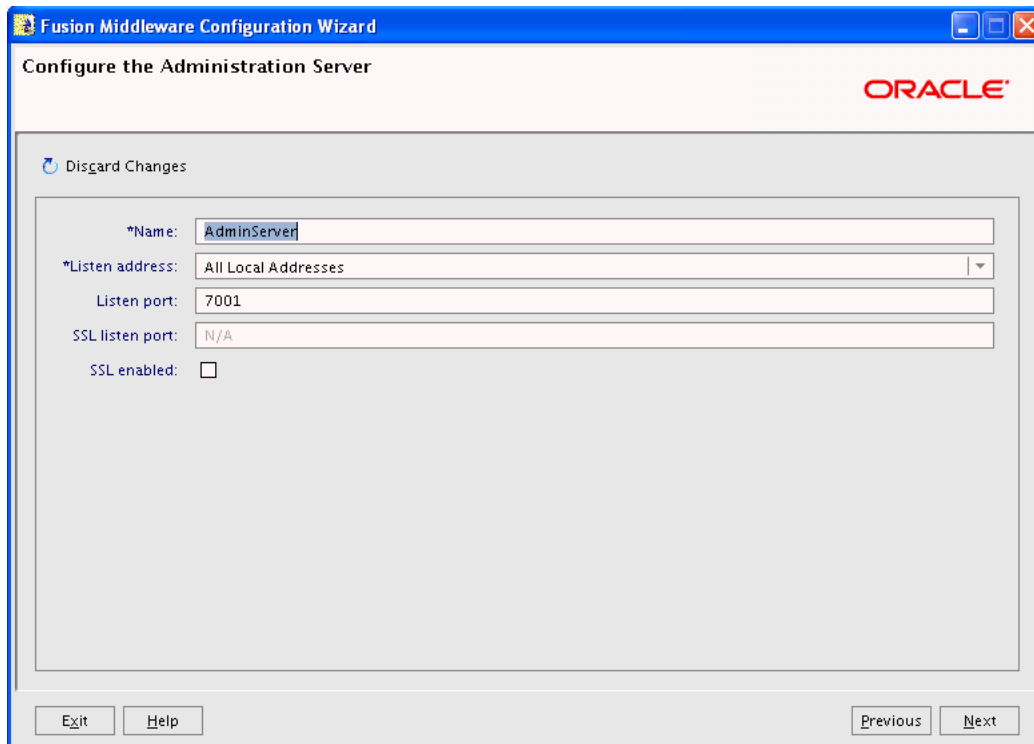
Use this screen to change the default configuration of the Administration Server for an Oracle WebLogic Server domain. Each domain must have one Administration Server, which hosts the Oracle WebLogic Server Administration Console used to perform administration tasks.

For the Administration Server, you can change values in these fields:

- **Name**

   Name of the Administration Server

- **Listen Address**

   An address on which the Administration Server will listen, selected from the list

- **Listen Port**

   Listen port number

- **SSL Listen Port**

   Port number for SSL connections, active when **SSL enabled** is selected

- **SSL Enabled**

   Enabled if selected and if a port number for SSL connections is provided in the **SSL Listen Port** field

Click **Next** to continue.

B.12 Configure Managed Servers
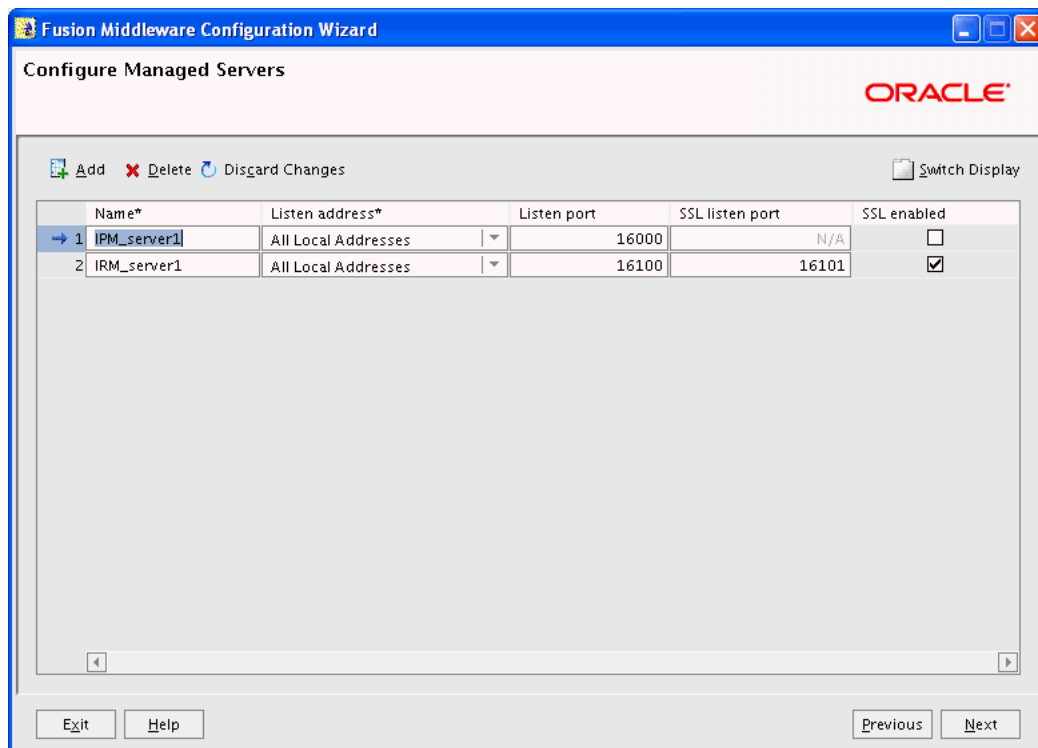
A Managed Server is an instance of Oracle WebLogic Server used to host enterprise applications. A typical production environment has at least one Managed Server.

Use this screen to change the default configuration of Managed Servers. For each Managed Server, you can change values in these columns:

- **Name**

  Name of the Managed Server

- **Listen Address**

  An address on which the server will listen, selected from the list

- **Listen Port**

  Listen port number

- **SSL Listen Port**

  Port number for SSL connections, active when **SSL enabled** is selected in the same row

- **SSL Enabled**

  Enabled if selected and if a port number for SSL connections is provided in the same row

Click **Next** to continue.

B.13 Configure Clusters
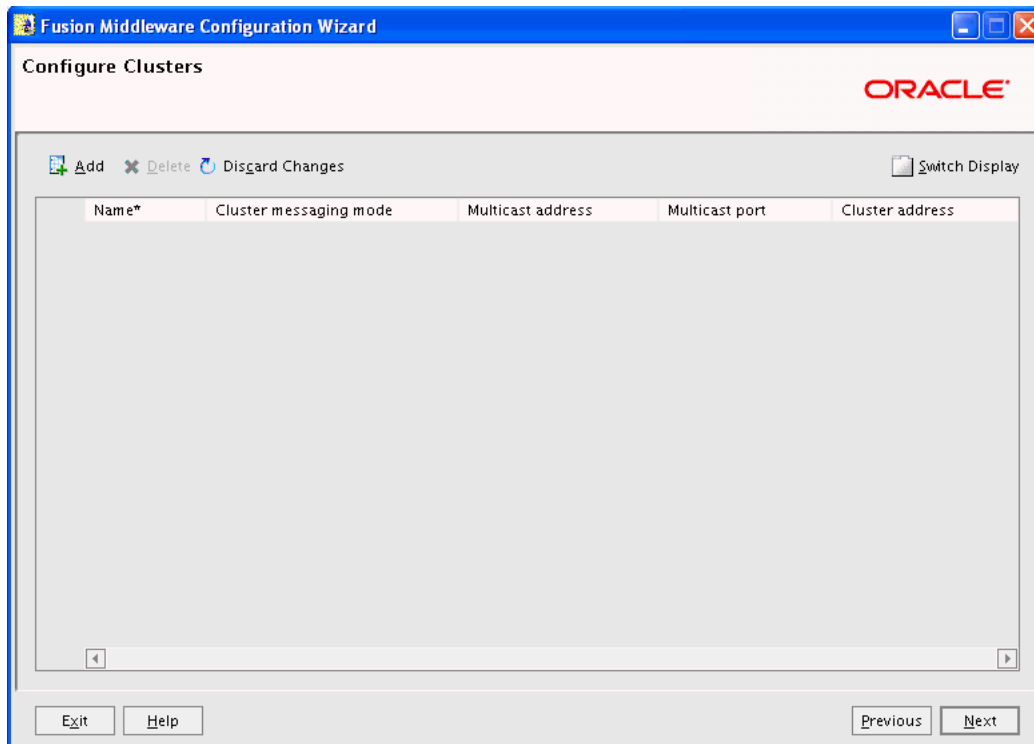
Use this screen to configure Oracle WebLogic Server clusters.

A cluster contains multiple Oracle WebLogic Server instances running simultaneously and working together for scalability and reliability. To clients, a cluster appears as a single Oracle WebLogic Server instance.

> **Notes:**
>
> - If you do not specify a cluster on the Configure Clusters screen, you cannot add Managed Servers later to create a cluster.
>
> - If you decide to enable a cluster, then you must assign a cluster address.

Click **Next** to continue.

B.14 Configure Machines
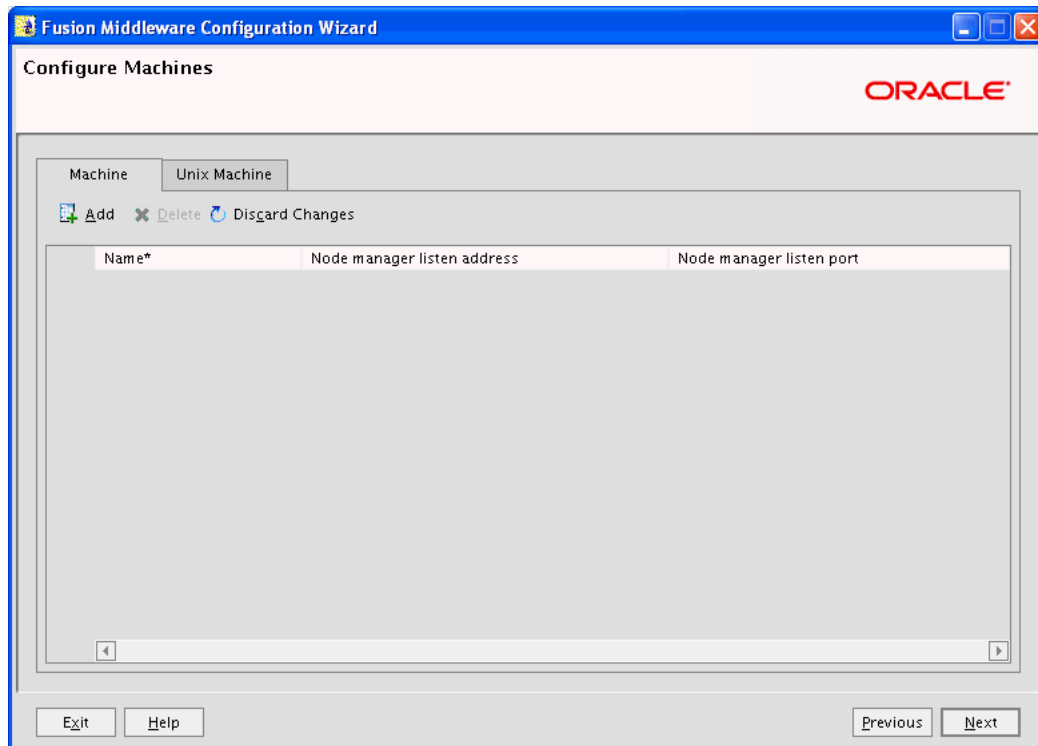
Use this screen to add or delete machines that host Oracle WebLogic Server instances.

The Administration Server and Node Manager use the machine configuration on this screen to start remote servers.

Click **Next** to continue.

B.15 Target Deployments to Clusters or Servers
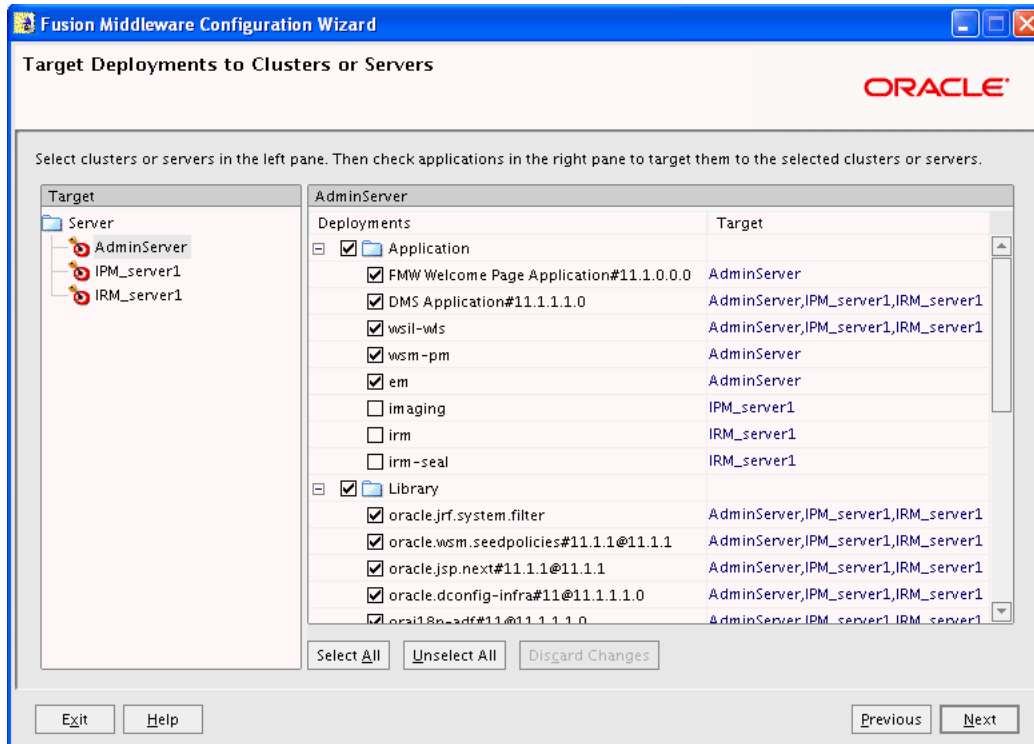
Use this screen to target your deployments to servers or clusters. Doing so enables Oracle WebLogic Server to serve the deployments to clients.

Click **Next** to continue.
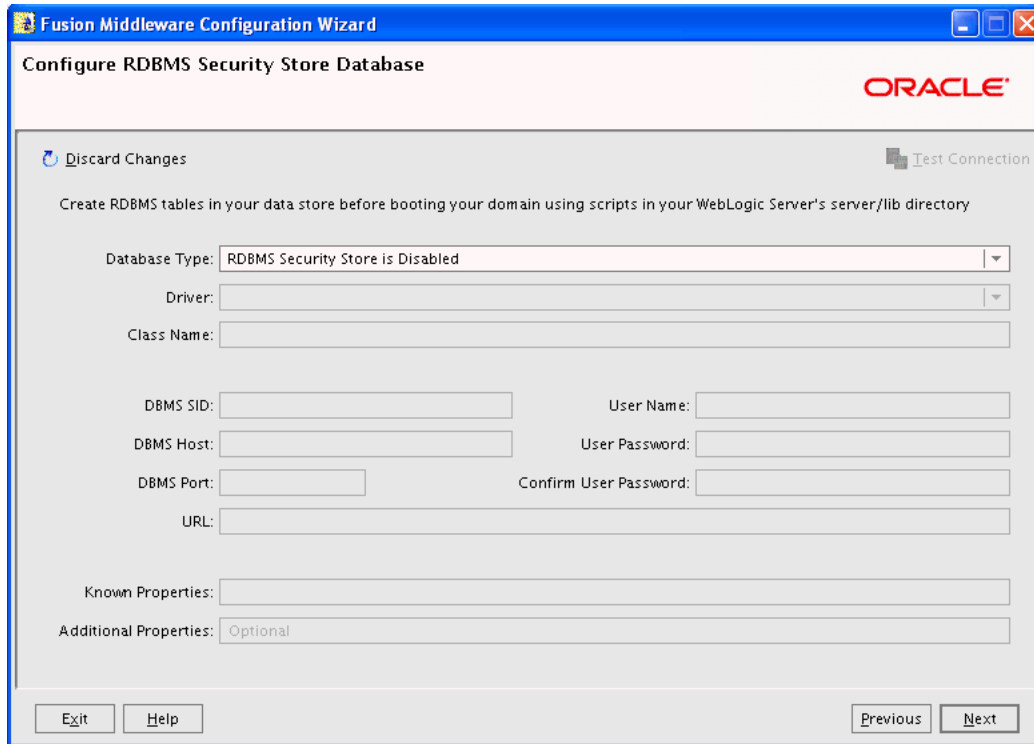
B.16 Target Services to Clusters or Servers
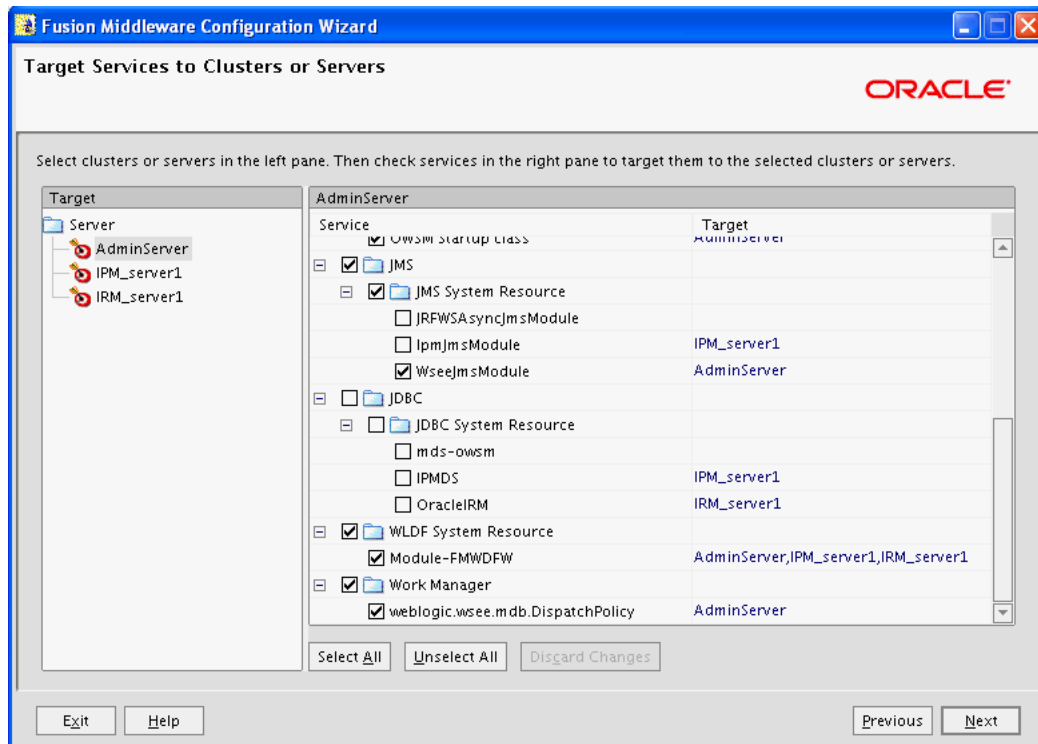
Use this screen to target your services (such as JMS and JDBC) to servers or clusters. Doing so enables your applications to use these services. For example, if you want to connect your application to Oracle WSM Policy Manager, you need to select **AdminServer** on the left and **mds-owsm** under **JDBC** and **JDBC System Resource** on the right.

Click **Next** to continue.

B.17 Configure RDBMS Security Store Database

Use this screen to make changes to your security store. Make sure that your RDBMS tables are created prior to booting your domain. The scripts used by the DBA are located in `server/lib` directory under the Oracle WebLogic Server home directory.

Click **Next** to continue.

B.18 Configure Key Store Credentials

Use this screen to specify passwords for Oracle Information Rights Management (Oracle IRM) and the Oracle Enterprise Manager plug-in for Oracle IRM.

B.19 Configuration Summary
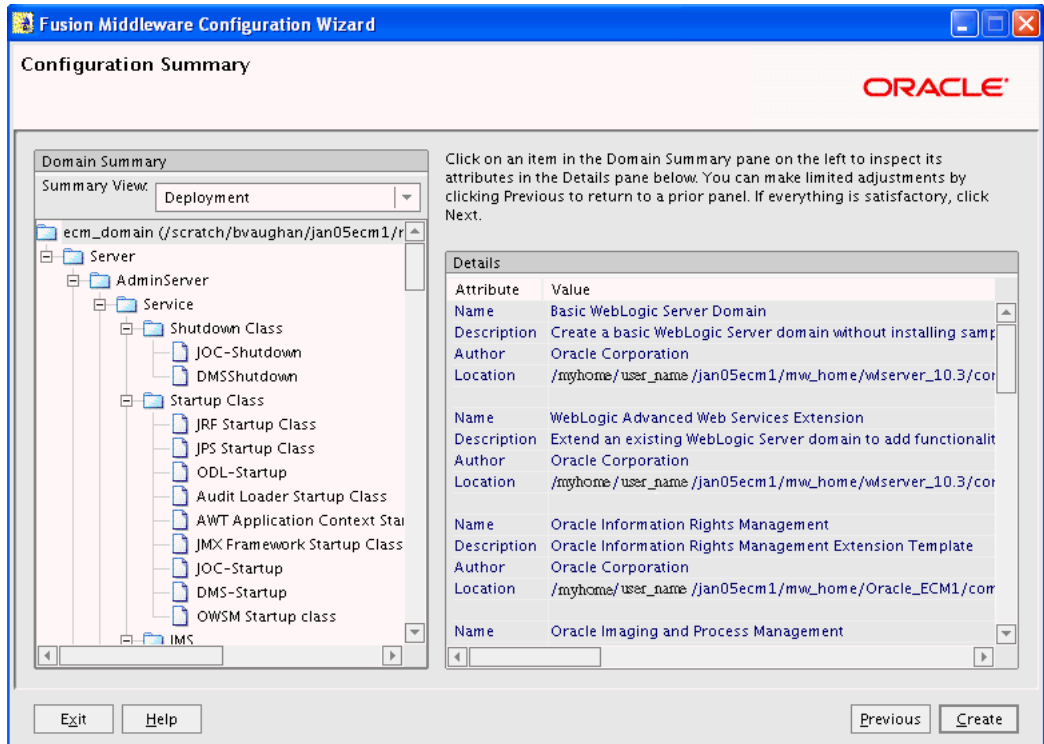
Review the contents of your domain.

Click **Previous** to go back and change something on a preceding screen.

Click **Next** to continue.

B.20 Creating Domain
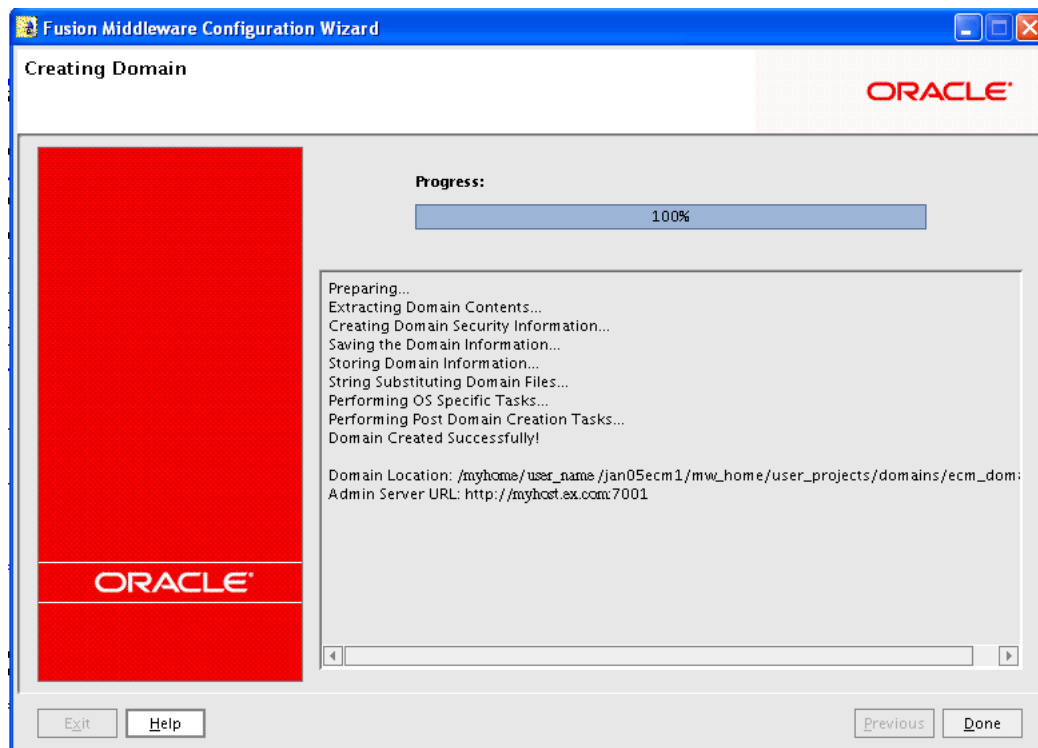
This screen shows the progress of the domain creation.

When the **Progress** bar shows 100%, click **Done** to dismiss the window.

B.21 Creating Domain (Extended Domain)
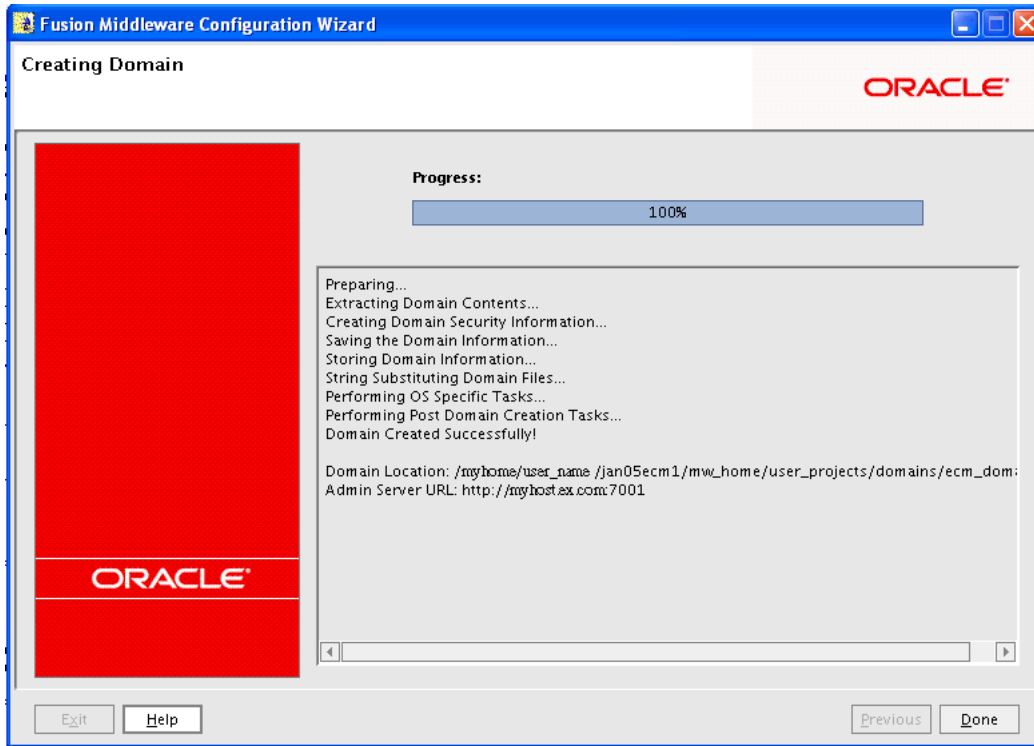
This screen shows the progress of the domain extension.

When the **Progress** bar shows 100%, click **Done** to dismiss the window.

C

Deinstallation Screens

This appendix describes the screens for deinstalling Oracle Enterprise Content Management Suite:

- Welcome
- Deinstall Oracle Home
- Deinstallation Progress
- Deinstallation Complete

C.1 Welcome
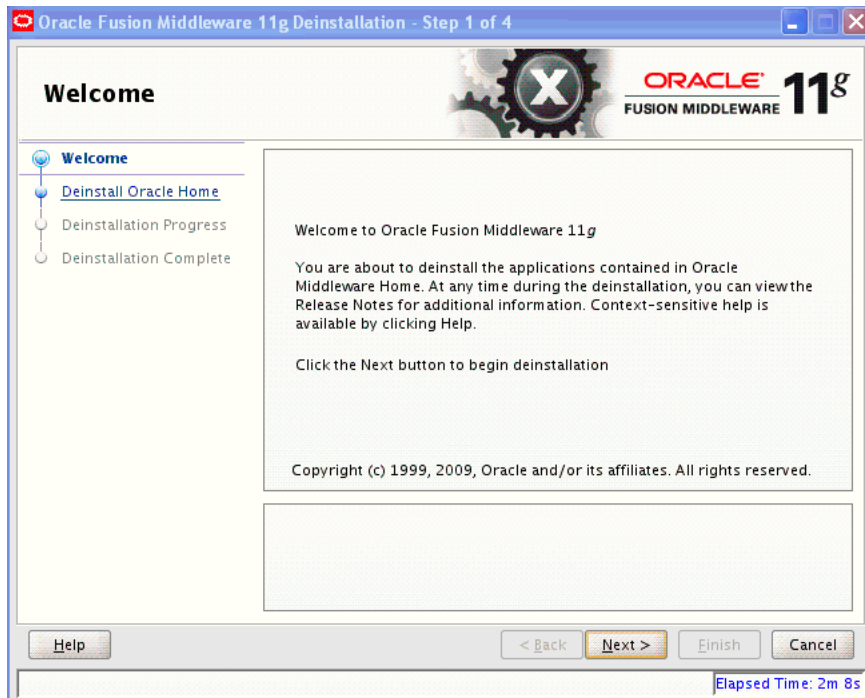
The Welcome screen is displayed each time you start the deinstaller.

Click **Next** to continue.

C.2 Deinstall Oracle Home
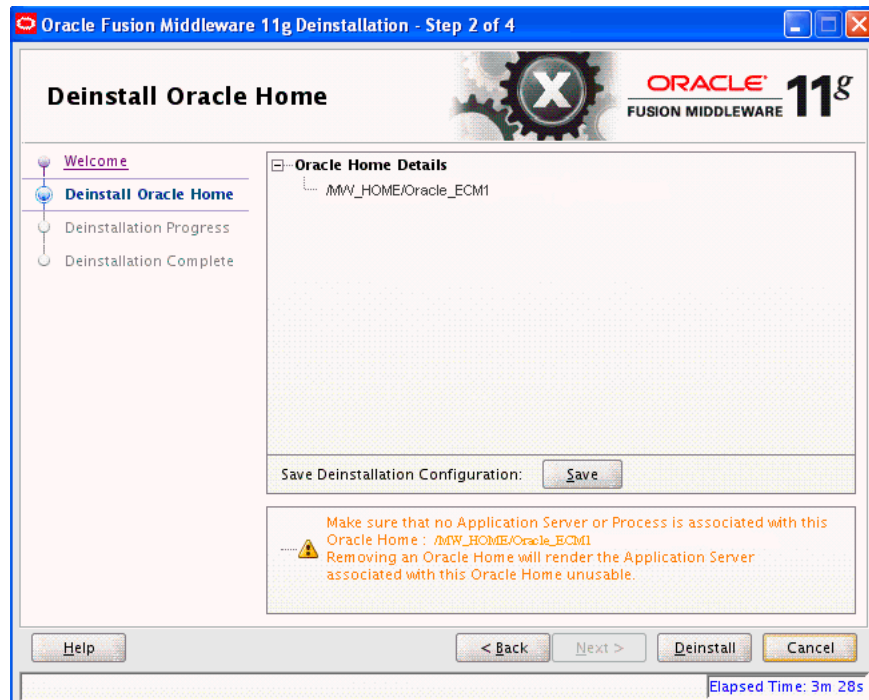
This screen shows the Oracle home directory that is about to be deinstalled. This is the Oracle home directory from which the deinstaller was started.

> **Note:**   Before you choose to remove this Oracle home, make sure that it is not in use by an existing domain.

Verify that this is the correct directory, then click **Deinstall** to continue.

C.3 Deinstallation Progress
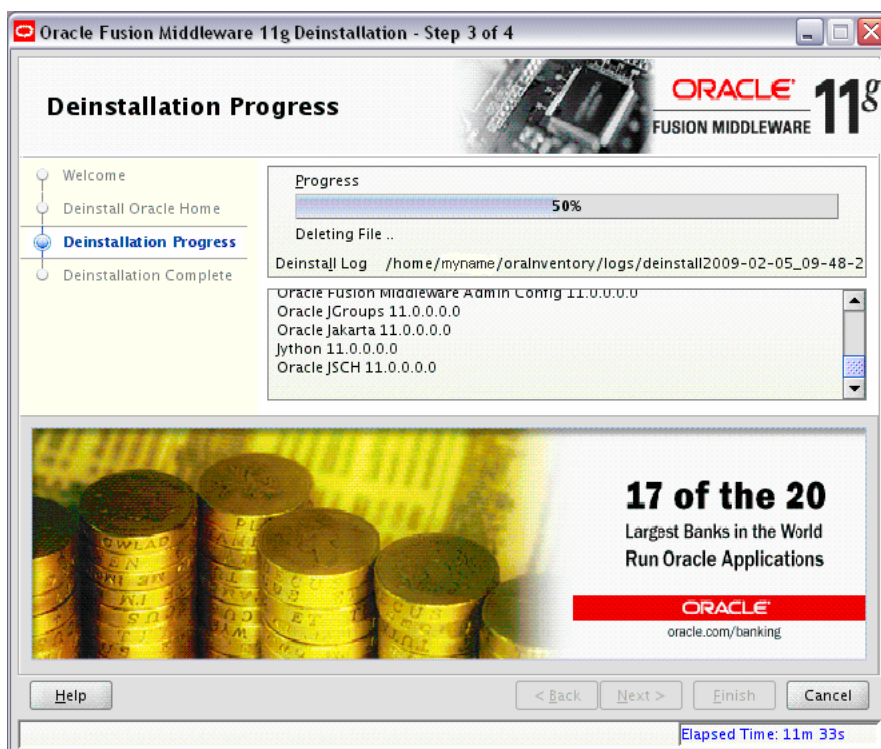
This screen shows you the progress of the deinstallation.

If you want to quit before the deinstallation is completed, click **Cancel**.

C.4 Deinstallation Complete
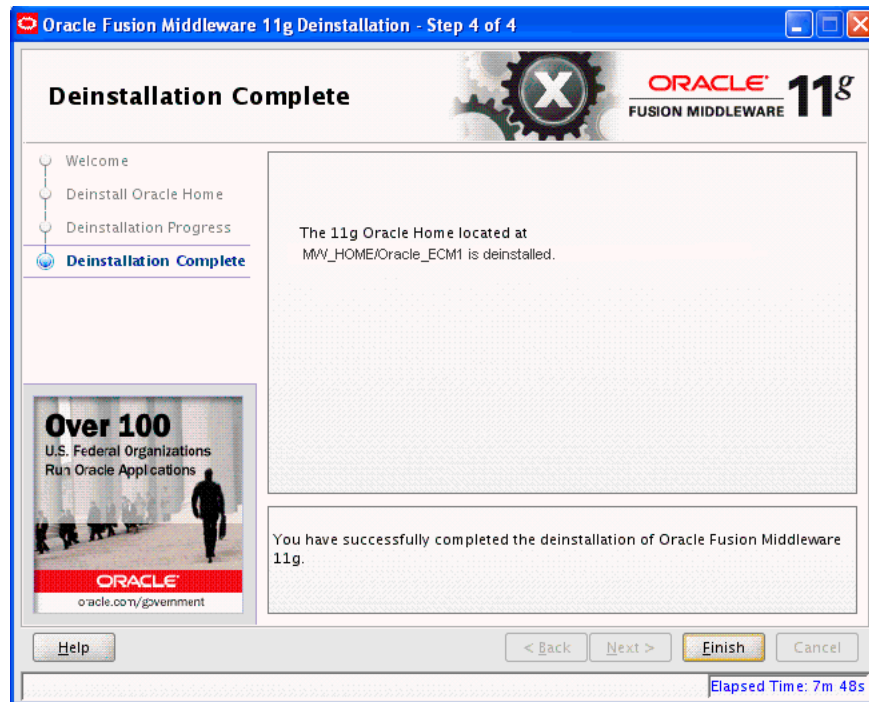
This screen summarizes the deinstallation that was just completed.

Click **Finish** to dismiss the screen.

D

Troubleshooting

This appendix provides troubleshooting information.

This appendix includes the following sections:

- Section D.1, "General Troubleshooting Tips"
- Section D.2, "Suite Installation and Configuration Troubleshooting"
- Section D.3, "Additional Help"

D.1 General Troubleshooting Tips

If you encounter an error during installation:

- Read the *Oracle Fusion Middleware Release Notes for Microsoft Windows (32-Bit)* for the latest updates. The release notes are available with the platform-specific documentation. The most current version of the release notes is available from the Oracle Documentation page on Oracle Technology Network at

  http://www.oracle.com/technology/documentation

- Verify that your system meets the requirements specified in Section 3.1.1, "Meeting System Requirements".

- If you are installing a middle tier, check that the OracleAS Infrastructure with which you want to associate the middle tier is running during installation.

- If you entered incorrect information on one of the installation screens, return to that screen by clicking **Back** until you see the screen.

- If an error occurred while the installer is copying or linking files:

  1. Note the error and review the installation log files.

  2. Remove the failed installation by following the steps in Chapter 8, "Deinstalling Oracle Enterprise Content Management Suite."

  3. Correct the issue that caused the error.

  4. Restart the installation.

D.2 Suite Installation and Configuration Troubleshooting

This section contains solutions to common problems that you might encounter while installing and configuring Oracle Enterprise Content Management Suite.

D.3 Additional Help

If this appendix does not solve the problem you encountered, try these other sources:

- *Oracle Fusion Middleware Release Notes for Microsoft Windows (32-Bit)*, available through the Oracle Documentation page on Oracle Technology Network at

  http://www.oracle.com/technology/documentation

- My Oracle Support (formerly Oracle*MetaLink*) Web site at

  http://support.oracle.com

If you do not find a solution for your problem, open a service request.

Index