Oracle® WebCenter Content

Installation Guide

11*g* Release 1 (11.1.1)

E14495-07

November 2011

ORACLE®

Oracle WebCenter Content Installation Guide 11g Release 1 (11.1.1)

E14495-07

Primary Author: Bonnie Vaughan

Contributing Authors: Sean Cearley, Sarah Howland, Kevin Hwang, Karen Johnson, Bruce Silver, Len Turmel, Jean Wilson, Martin Wykes

Contributors: Tom Albrecht, Satheesh Amilineni, Pete Chapman, Sandra Christiansen, Eric Cloney, Rupesh Das, Carl Foster, Sudhanshu Garg, Brian Gray, Helen Grembowicz, Marsha Hancock, MaryJo Hoepner, Mei Hong, David Jones, Vasant Kumar, Peter LaQuerre, Bill Loi, Rene Madsen, Liju Nair, John Neely, Saskia Nehls, Bob O'Kane-Trombley, Alejandro Paredes, Ty Paywa, Andy Peet, Sancho Pinto, Wes Prichard, Rafael Ramirez, Indira Smith, Gene Sutay, Vani Srivastava, David Tom, David Truckenmiller, Matt Wall, Venkatesh Yadalam, Lisa Zitek-Jones

Contents

3 Configuring Oracle WebCenter Content Applications

4   Completing the WebCenter Content Configuration

5   Completing the Inbound Refinery Configuration

6   Completing the Imaging Configuration

7   Completing the Oracle IRM Configuration

C Deinstallation Screens for Oracle WebCenter Content

D Silent Installation

E Troubleshooting

Index

Preface

This installation guide provides information and instructions for installing, configuring, and troubleshooting Oracle WebCenter Content.

Audience

This guide is intended for users who are installing Oracle WebCenter Content 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

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

Access to Oracle Support

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

Related Documents

For 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 Portal*

- *Oracle Fusion Middleware Application Security Guide*

- *Oracle Fusion Middleware Concepts*

- *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard*

- *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle WebCenter Content*

- *Oracle Fusion Middleware High Availability Guide*

- *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*

- *Oracle Fusion Middleware Installation Guide for Oracle SOA Suite and Oracle Business Process Management Suite*

- *Oracle Fusion Middleware Installation Guide for Oracle Web Tier*

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

- *Oracle Fusion Middleware Installation Planning Guide*

- *Oracle Fusion Middleware Java EE Developer's Guide for Oracle Application Development Framework*

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

- *Oracle Fusion Middleware Patching Guide*

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

- *Oracle Fusion Middleware Securing Oracle WebLogic Server*

- *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*

- *Oracle WebCenter Content Administrator and Manager's Guide for Site Studio*

- *Oracle WebCenter Administrator's Guide for Application Adapters*

- *Oracle WebCenter Content Administrator's Guide for Conversion*

- *Oracle WebCenter Content Administrator's Guide for Imaging*

- *Oracle WebCenter Content Administrator's Guide for Records*

- *Oracle WebCenter Content Quick Installation Guide*

- *Oracle WebCenter Content System Administrator's Guide for Content Server*

- *Oracle WebCenter Content Technical Reference Guide for Site Studio*

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

- *Oracle WebCenter Content User's Guide for Desktop*

- *Oracle WebCenter Content User's Guide for Records*

- *Oracle WebCenter Content User's Guide for Site Studio Designer*

Conventions

In this document, the term **UNIX operating system** or **UNIX system** refers to a category of operating systems that includes Linux operating systems. Most UNIX command examples in this document are for use with the Bourne shell. You should use the equivalent commands for the shell you are using.

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 WebCenter Content, 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 WebCenter Content and configuring its products as applications deployed to an Oracle WebLogic Server domain.

This chapter includes the following sections:

- Section 1.1, "Oracle WebCenter Content Applications"
- Section 1.2, "Installation Roadmap"
- Section 1.3, "Topology Summary for Oracle WebCenter Content"

1.1 Oracle WebCenter Content Applications

Oracle WebCenter Content includes the following products:

- **Oracle WebCenter Content (WebCenter Content)**

  WebCenter Content, which includes Oracle WebCenter Content Server, provides a unified application for several different types of content management.

- **Oracle WebCenter Content: Inbound Refinery (Inbound Refinery)**

  Inbound Refinery is a conversion server that manages file conversions for electronic assets such as documents, digital images, and motion video. In addition to conversion, Inbound Refinery provides thumbnail functionality for documents and images, storyboarding for video, and the ability to extract and use EXIF data from digital images and XMP data from electronic files generated from programs such as Adobe Photoshop and Adobe Illustrator. You can use Inbound Refinery to convert content items stored in Content Server.

- **Oracle WebCenter Content: Imaging (Imaging)**

  Imaging 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 WebCenter Content: Rights Desktop software is required on every end user device on which sealed information is created or used.

- **Oracle WebCenter Content: Records (Records)**

  Records manages content items on a retention schedule, which determines the life cycle of each content item. Records combines both records management and retention management into one software system. You can use Records to track and preserve content as needed, or to dispose of content when it is no longer required.

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. You cannot configure an Oracle WebCenter Content 11.1.1.6.0 application in an Oracle WebLogic Server domain that already has an Oracle Enterprise Content Management Suite application from an earlier release installed.

1.2 Installation Roadmap

The process of installing and configuring Oracle WebCenter Content includes these high-level tasks:

1. Preparing your system environment for installation

2. Creating schemas for applications

3. Installing an Application Server and Oracle Fusion Middleware

4. Installing Oracle WebCenter Content

5. Configuring Oracle WebCenter Content

6. Installing and configuring an external LDAP-based identity store

7. Performing Postinstallation Configuration

8. Verifying the Configuration

Figure 1–1 shows these steps in the installation process.

Figure 1–1   Roadmap for Installing and Configuring Oracle WebCenter Content
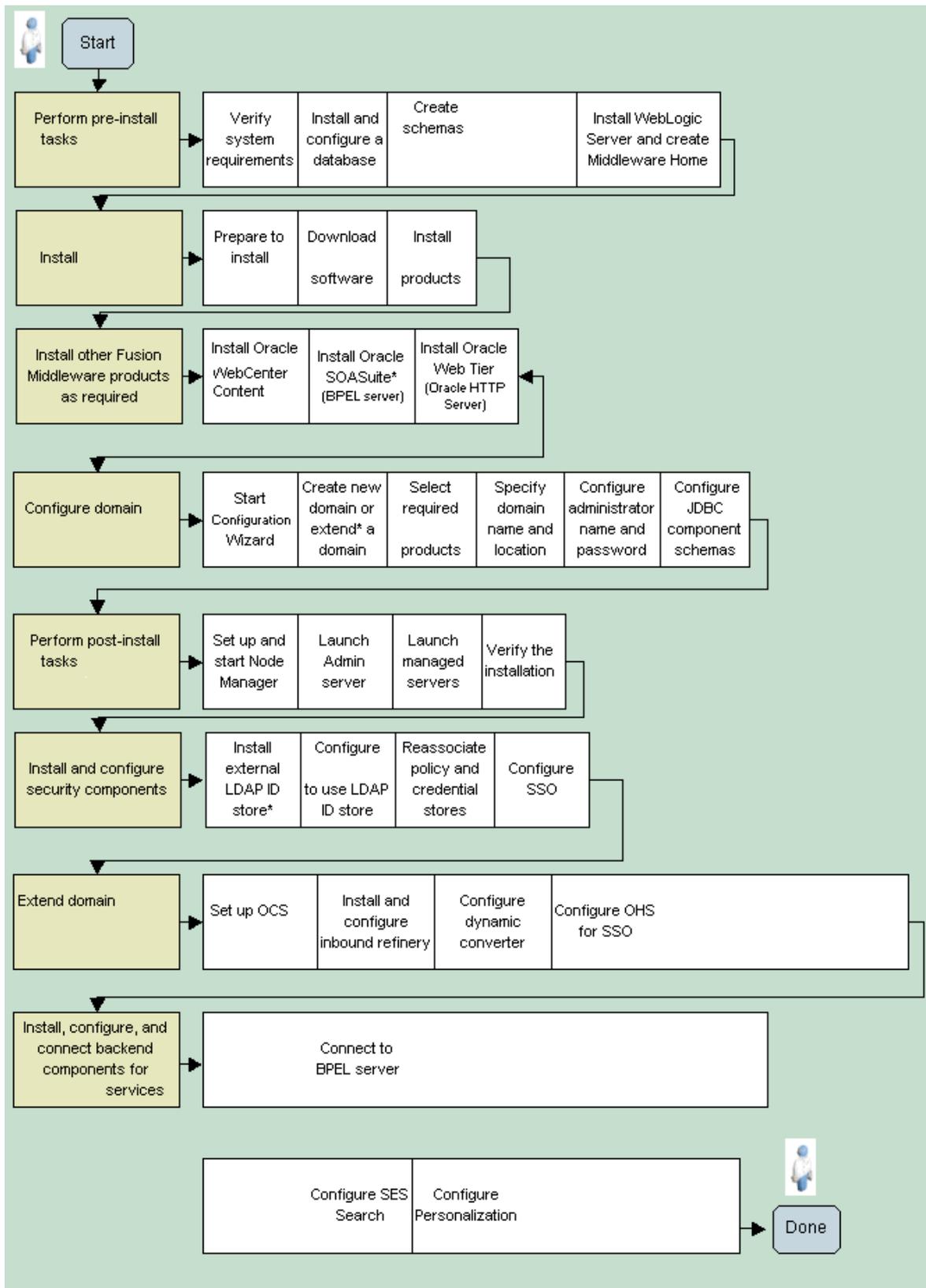
Table 1–1 describes the high-level tasks for installing and configuring Oracle WebCenter Content. You need to perform the tasks in order except as noted. The table also shows where to get more information about each task.

Table 1–1   Oracle WebCenter Content Installation Procedure

Task	Description	Optional	More Information
1. Preparing for installation	Ensure that your system environment meets the general installation requirements for Oracle Fusion Middleware, for Oracle WebCenter Content, and for Repository Creation Utility (RCU), which requires a supported database.	No	Section 2.1, "Preparing to Install."
2. Creating schemas for applications	Oracle WebCenter Content applications require schemas that must be installed in a supported database, such as Oracle Database, Microsoft SQL Server, or IBM DB2. Prepare a database for Oracle WebCenter Content schemas, then install RCU and use it to create schemas. **Note:** You can perform this task before or after task 3, "Installing an application server and Oracle Fusion Middleware" and task 4, "Installing Oracle WebCenter Content."	No	Section 2.1.4, "Installing and Configuring a Supported Database" Section 2.2, "Creating Oracle WebCenter Content Schemas with the Repository Creation Utility"
3. Installing an application server and Oracle Fusion Middleware	Oracle WebCenter Content runs on Oracle WebLogic Server. You must install Oracle WebLogic Server, or a supported third-party application server, before you install Oracle WebCenter Content. The Oracle WebLogic Server 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, "Creating schemas for applications."	No	Section 2.3, "Installing an Application Server and Oracle Fusion Middleware"
4. Installing Oracle WebCenter Content	Use the Oracle Fusion Middleware 11*g* WebCenter Content Installer to install Oracle WebCenter Content. The installer creates an Oracle home directory named `Oracle_ECM1`, where it installs the Oracle WebCenter Content products. The installer lays down the Oracle WebCenter Content binaries for these products: ■ Imaging ■ Oracle IRM ■ WebCenter Content ■ Records ■ Inbound Refinery **Note:** You can perform this task before or after task 2, "Creating schemas for applications," but you need to perform it after task 3, "Installing an application server and Oracle Fusion Middleware."	No	Chapter 2, "Installing Oracle WebCenter Content"

Table 1–1   (Cont.) Oracle WebCenter Content Installation Procedure

Task	Description	Optional	More Information
5. Configuring Oracle WebCenter Content	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 as `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 WebCenter Content products as applications.	No	Chapter 3, "Configuring Oracle WebCenter Content Applications"
6. Installing and configuring an external LDAP-based identity store	By default, Oracle WebCenter Content 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. In a production system, Oracle WebCenter Content applications need to use an external Lightweight Directory Application Protocol (LDAP) authentication provider rather than the Oracle WebLogic Server embedded LDAP server. To manage the identities of users across diverse servers and enable single sign-on across applications, you must install and configure an external LDAP-based identity store. **Note:** If you perform this task before task 7, "Performing Postinstallation Configuration" and task 8, "Verifying the Configuration," the postinstallation configuration is easier.	Yes for Oracle WebLogic Server No for an IBM WebSphere application server	Section 3.9, "Reassociating the Identity Store with an External LDAP Authentication Provider."
7. Performing Postinstallation Configuration	For each Oracle WebCenter Content 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.	No	Chapter 4, "Completing the WebCenter Content Configuration" Chapter 5, "Completing the Inbound Refinery Configuration" Chapter 6, "Completing the Imaging Configuration" Chapter 7, "Completing the Oracle IRM Configuration" Chapter 8, "Completing the Records Configuration"

Table 1–1   (Cont.) Oracle WebCenter Content Installation Procedure

Task	Description	Optional	More Information
8. Verifying the Configuration	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 WebCenter Content 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.	No	Chapter 9, "Verifying the Oracle WebCenter Content Configuration"

1.2.1 Installation Modules

The following installation modules are required for installing the products in Oracle WebCenter Content:

- Oracle Fusion Middleware and Oracle WebLogic Server Homes

- Database

- Repository Creation Utility

- Oracle WebCenter Content

1.2.1.1 Oracle Fusion Middleware and Oracle WebLogic Server Homes

Oracle WebCenter Content requires a Middleware home and an application 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 2.3, "Installing an Application Server and Oracle Fusion Middleware."

If the application server you want to use is an IBM WebSphere Application Server, see "Managing Oracle WebCenter Content on IBM WebSphere Application Servers" in the *Oracle Fusion Middleware Third-Party Application Server Guide*.

1.2.1.1.1   Middleware Home, Oracle Common Homes, and Oracle homes 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
    coherence_3.7
    jdk160_29
    jrockit_160_29_D1.2.0-10
    logs
    modules
    wlserver_10.3
    oracle_common
    utils
    WC_CONTENT_ORACLE_HOME
    user_projects
```

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). The default Middleware home is in the user's home directory, *user_home*/Oracle/Middleware on a UNIX operating system or *user_home*\Oracle\Middleware on a Windows operating system.

MW_HOME represents the location of a Middleware home in path names. For more information, see "Middleware Home and WebLogic Home Directories" in the *Oracle Fusion Middleware Installation Planning Guide*.

The WebCenter Content Oracle home contains the binary and library files necessary for Oracle WebCenter Content. *WC_CONTENT_ORACLE_HOME* represents the WebCenter Content Oracle home in path names. The default WebCenter Content Oracle home is *MW_HOME*/Oracle_ECM1 on a UNIX operating system or *MW_HOME*\Oracle_ECM1 on a Windows operating system.

The WebCenter Content 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 Fusion Middleware Control and Java Required Files (JRF).

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

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

A domain is the basic administrative unit of Oracle WebLogic Server. Each consists of one or more Oracle WebLogic Server instances and logically related resources and services that are managed collectively as one unit.

Figure 1–2 shows the structure of a domain, with an Administration Server, Managed Servers, and Managed Server clusters.

Figure 1–2   Oracle WebLogic Server Domain Structure
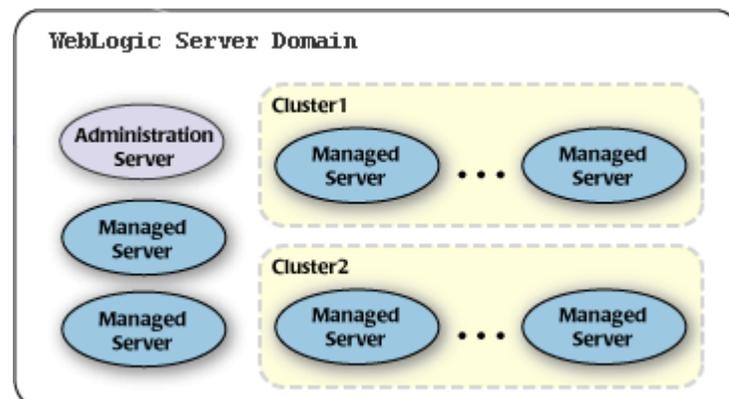
After you create a domain, you can use the Oracle WebLogic Server Administration Console or Fusion Middleware Control to perform postinstallation tasks on the domain. You can also use Oracle WebLogic Scripting Tool (WLST) commands to perform some of the postinstallation tasks.

1.2.1.2 Database

The configuration of Oracle WebCenter Content 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 Oracle WebCenter Content.

The overall performance of a WebCenter Content system is dependent on the speed at which files that are checked into the server can be stored and retrieved. Using a database to store the files that are stored in the server requires that the database can execute both Read and Write commands at speeds similar to a file system. Oracle Secure Files meets this standard. For databases other than Oracle Database, consult your database provider to ensure that the database can achieve your storage and retrieval requirements.

For more information, see Section 2.1.4, "Installing and Configuring a Supported Database."

1.2.1.3 Repository Creation Utility

You need to install and run Repository Creation Utility (RCU) to create a database schema for each Oracle WebCenter Content 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 operating system to create schemas in a supported database installed on any operating system.

For information about installing and running RCU, see Section 2.2, "Creating Oracle WebCenter Content Schemas with the Repository Creation Utility."

1.2.1.4 Oracle WebCenter Content

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

1.2.2 Software Downloads for Oracle WebCenter Content Installation and Configuration

You can download the software required for installing and configuring Oracle WebCenter Content from either of two web sites:

- Oracle Software Delivery Cloud
- Oracle Technology Network (OTN)

1.2.2.1 Downloading Software from Oracle Software Delivery Cloud for Installing and Configuring Oracle WebCenter Content

You can use the Oracle Software Delivery Cloud web site to download products for which you have purchased a license.

To download software from Oracle Software Delivery Cloud for installing and configuring Oracle WebCenter Content:

1. Go to the Oracle Software Delivery Cloud web site at

   http://edelivery.oracle.com

2. On the Welcome page, click **Continue**.

3. Enter your user information, and click **Continue**.

4. Select the Oracle Fusion Middleware product pack and your installation platform, and then click **Go**.

5. From the list of media packs, select the one for Release 11.1.1.6.0, which includes Oracle WebCenter Content.

6. Click the **Description** link to display a list of downloadable ZIP files for the media pack.

   Each ZIP file has a unique part number.

7. Click the **Readme** button at the top of the list for instructions on which files to download for your product licenses.

1.2.2.2 Downloading Software from OTN for Installing and Configuring Oracle WebCenter Content

You can download Oracle WebLogic Server 11*g*R1 (10.3.5 or 10.3.6), Oracle Database, Repository Creation Utility, and Oracle WebCenter Content software from Oracle Technology Network (OTN).

To download software from OTN for installing and configuring Oracle WebCenter Content:

1. If you do not have Oracle WebLogic Server 11*g*R1 (10.3.5 or 10.3.6) on your system, you can download it from the Oracle WebLogic Server Downloads page on OTN at

   `http://www.oracle.com/technetwork/middleware/weblogic/downloads/ind
   ex.html`

   Download Oracle WebLogic Server 11*g*R1 (10.3.5 or 10.3.6) for your platform.

2. If you need Oracle Database, you can download it from the Oracle Database Software Downloads page on OTN at

   `http://www.oracle.com/technology/software/products/database/index.h
   tml`

   Download Oracle Database 11*g* for your platform.

   Instead of Oracle Database, you can use Microsoft SQL Server or IBM DB2. For information about database versions supported by Repository Creation Utility and Oracle WebCenter Content, 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`

3. For the Oracle WebCenter Content media and the corresponding version of Repository Creation Utility, go to the Oracle Fusion Middleware 11*g* Software Downloads page on OTN at

   `http://www.oracle.com/technology/software/products/middleware/htdoc
   s/fmw_11_download.html`

   If you are using Imaging with Oracle BPEL Process Manager and Oracle Application Extension Framework (AXF), preinstallation requirements include installing Oracle SOA Suite 11*g* as well as Oracle JDeveloper and Oracle Application Development Framework 11*g*. On the Oracle Fusion Middleware 11*g* Software Download page, download the following software:

   ■ **SOA Suite (11.1.1.6.0)** under Runtime Software

   ■ **JDeveloper and Application Development Framework (11.1.1.6.0)** under Required Additional Software

      After Oracle JDeveloper is installed, you must install the Oracle SOA Suite Design-Time Components. Oracle SOA Suite is not automatically installed

with Oracle JDeveloper. Before you can create a SOA application and project, you must install the Oracle SOA Suite Extension for JDeveloper.

1.3 Topology Summary for Oracle WebCenter Content

When you install Oracle WebLogic Server, the Oracle WebLogic Server 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 Fusion Middleware Control and Java Required Files (JRF).

When you install Oracle WebCenter Content, a WebCenter Content Oracle home directory (*WC_CONTENT_ORACLE HOME*) is created under the Middleware home directory. The WebCenter Content Oracle home directory contains the binary and library files for Oracle WebCenter Content.

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

- WebCenter Content Managed Server

- Records Managed Server

- Inbound Refinery Managed Server

- Imaging Managed Server

- Oracle IRM Managed Server

Figure 1–3 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 1–3   Topology of an Oracle WebCenter Content Installation
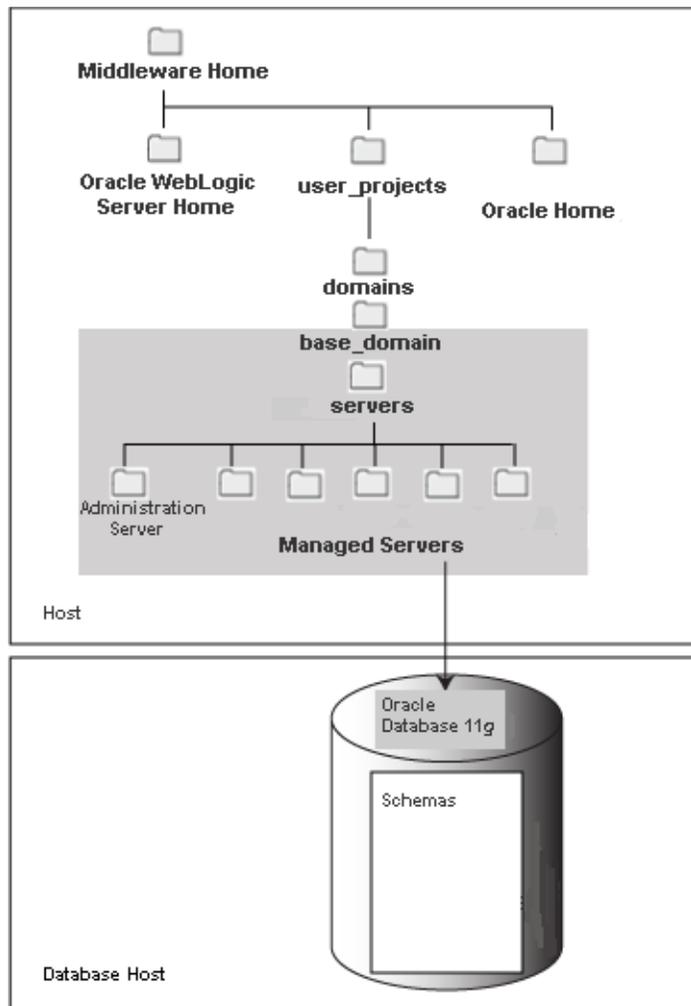
The topology in Figure 1–3 includes multiple applications configured on the same host in one Oracle WebLogic Server domain that includes only Oracle WebCenter Content applications. The schemas for the applications are in the same database.

2

Installing Oracle WebCenter Content

This chapter explains how to install the Oracle WebCenter Content component of Oracle Fusion Middleware.

This chapter includes the following sections:

2.1 Preparing to Install

Before you install Oracle WebCenter Content, you need to verify that your system meets the installation requirements and set environment variables. If your system does not have an application server and Oracle Fusion Middleware installed, you need to install them and create a new Middleware home.

To provide accessibility on a Windows operating system, you can also install Java Access Bridge. For more information, see "Installing and Configuring Java Access Bridge (Windows Only)" in the *Oracle Fusion Middleware Installation Planning Guide*.

2.1.1 Disabling the 8.3 File Naming Convention on a Windows Operating System

Before you install Oracle WebCenter Content on a Windows Operating System, you need to disable the 8.3 file naming convention (maximum 8-character file name and 3-character extension).

If the WebCenter Content `weblayout` directory is on a file system with 8.3 semantics, the legacy 16-bit 8.3 file names will conflict with revision labels and cause file loss.

To disable the 8.3 file naming convention on a Windows Operating System:

1. Open the Windows Registry Editor (`regedit`), and go to the following key:

   `HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control/FileSystem`

2. Set the value of the `NtfsDisable8dot3NameCreation` key to 1.

3. Restart the Windows operating system for the change to take effect.

2.1.2 Enabling Unicode Support

Your operating system configuration can influence the behavior of characters supported by Oracle WebCenter Content.

On a UNIX operating system, Oracle highly recommends that you enable Unicode support by setting the `LANG` and `LC_ALL` environment variables to a locale with the UTF-8 character set. This enables the operating system to process any character in Unicode. Web technologies are based on Unicode.

If the operating system is configured to use a non-UTF-8 encoding, Oracle WebCenter Content components may function in an unexpected way. For example, a non-ASCII file name can make the file inaccessible and cause an error. Oracle does not support problems caused by operating system constraints.

2.1.3 Reviewing System Requirements and Certification

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.

Notes:

- 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.

- For a 64-bit Linux operating system, you should use the 32-bit Java Runtime Environment (JRE) on a client machine for the Imaging Advanced Viewer.

- For the IBM JDK with Oracle WebCenter Content and WebSphere Application Server, certain functionality, such as the check for patches feature, will not work correctly unless the Java socket factories are changed. The IBM JRE has its own Secure Sockets Layer (SSL) socket factories. For more information, see "Changing Java Socket Factories in the IBM JDK" in the *Oracle Fusion Middleware Third-Party Application Server Guide*.

2.1.4 Installing and Configuring a Supported Database

The database that you use for Oracle WebCenter Content applications must be compatible with Repository Creation Utility (RCU), which creates the schemas for the Oracle WebCenter Content applications. For more information, see Section 2.2, "Creating Oracle WebCenter Content Schemas with the Repository Creation Utility."

> **Note:** RCU is available only for 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 Documentation page on Oracle Technology Network at

http://www.oracle.com/technetwork/indexes/documentation/index.html#database

2.1.5 Providing the Location of the 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 the 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 the 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 following script as the `root` user:

   ```
   inventory_directory/createCentralInventory.sh
   ```

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

2.1.6 Creating a Symbolic Link to the chmod Command on a Solaris System

Before installing Oracle WebCenter Content 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.

2.2 Creating Oracle WebCenter Content Schemas with the Repository Creation Utility

This section explains how to use Repository Creation Utility (RCU) to create database schemas for Oracle WebCenter Content applications, in these topics:

- Preparing to Run RCU and Load Schemas

- Creating Schemas for Oracle WebCenter Content Applications

2.2.1 Preparing to Run RCU and Load Schemas

Oracle WebCenter Content 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.

2.2.1.1 Database Prerequisites

Installation of Oracle WebCenter Content 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 WebCenter Content products.

For information about supported databases, see the "System Requirements and Supported Platforms" 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

After you have installed a database, make sure that it is configured correctly by referring to the "Repository Creation Utility Requirements" section in the "System Requirements and Specification" document on Oracle Technology Network at

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

2.2.1.2 Database Maintenance for Oracle WebCenter Content Schemas

After the Oracle WebCenter Content schemas are created, make sure the database index is up to date. Add new indexes when necessary.

2.2.1.3 RCU for Linux and Windows Operating Systems

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

2.2.2 Creating Schemas for Oracle WebCenter Content Applications

Oracle WebCenter Content requires that an application schema exists in the database before configuration of the application. You must run the Repository Creation Utility (RCU) to create application schemas in the database, which must be up and running before you start RCU. You can create application schemas before or after you install Oracle WebLogic Server or Oracle WebCenter Content, for one or more of these applications:

- Oracle WebCenter Content (WebCenter Content, which includes Oracle WebCenter Content Server)

- Oracle WebCenter Content: Inbound Refinery (Inbound Refinery)

- Oracle WebCenter Content: Imaging (Imaging)

- Oracle Information Rights Management (Oracle IRM)

- Oracle WebCenter Content: Records (Records)

To create schemas for Oracle WebCenter Content applications:

1. Unzip a ZIP file containing the Repository Creation Utility, and then start RCU with the `bin/rcu` or `BIN\rcu.bat` file:

   - **UNIX path:** *RCU_HOME*`/bin/rcu`

   - **Windows path:** *RCU_HOME*`\BIN\rcu.bat`

   You can download a ZIP file containing the Repository Creation Utility from either of these web sites:

   - Oracle Software Delivery Cloud at

     http://edelivery.oracle.com/

   - Oracle Fusion Middleware 11*g* Software Downloads page on Oracle Technology Network (OTN) 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 start 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: Select `Oracle Database`, `Oracle Database enabled for edition-based redefinition`, `Microsoft SQL Server`, or `IBM DB2`.

The default is `Oracle Database`.

Before you can use SQL Server with WebCenter Content, you need to turn on snapshot isolation in the database. If you plan to use SQL Server for the back-end database for Imaging and Oracle SOA Suite, you also need to configure the Metadata Services (MDS) repository in the database and then create an MDS schema on the Select Components screen (Step 5).

The prerequisite configurations for WebCenter Content and the MDS repository follow:

a. Log in to the database with a user name that has DBA privileges and does not have multiple logins to the database.

Multiple logins for the DBA would result in a lock error.

b. Alter the database to turn on the `ALLOW_SNAPSHOT_ISOLATION` option, with this command:

```
ALTER DATABASE dbname SET ALLOW_SNAPSHOT_ISOLATION ON
```

c. Alter the database to turn on the `READ_COMMITTED_SNAPSHOT` option, with this command:

```
ALTER DATABASE MDS SET READ_COMMITTED_SNAPSHOT ON
```

For more information about supported databases, see Section 2.2.1.1, "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`.

  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 is `1521` for an Oracle Database instance, `1433` for Microsoft SQL Server, or `50000` for IBM DB2.

- **Service Name:** Specify the service name for the database. Typically, the service name is the same as the global database name.

  If you do not know the service name for your 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. Another way to find the service name is to log in to the database as `SYS` and run the following command:

```
show parameter service_name
```

  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 SYSDBA or DBA privileges. The default user name with SYSDBA privileges is `SYS`.

> For Microsoft SQL Server, specify the name of a user with SYSDBA or DBA privileges.
>
> For IBM DB2, RCU needs to connect as the MDS schema owner. Specify an operating system user for the MDS database schema (for example, `OWSM_MDS`). An operating system user has to be created before you use RCU to create an MDS schema in an IBM DB2 database.

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

> For IBM DB2, specify the password for the operating system user for the MDS database schema.

■ **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

Figure 2–1   RCU Select Components Screen
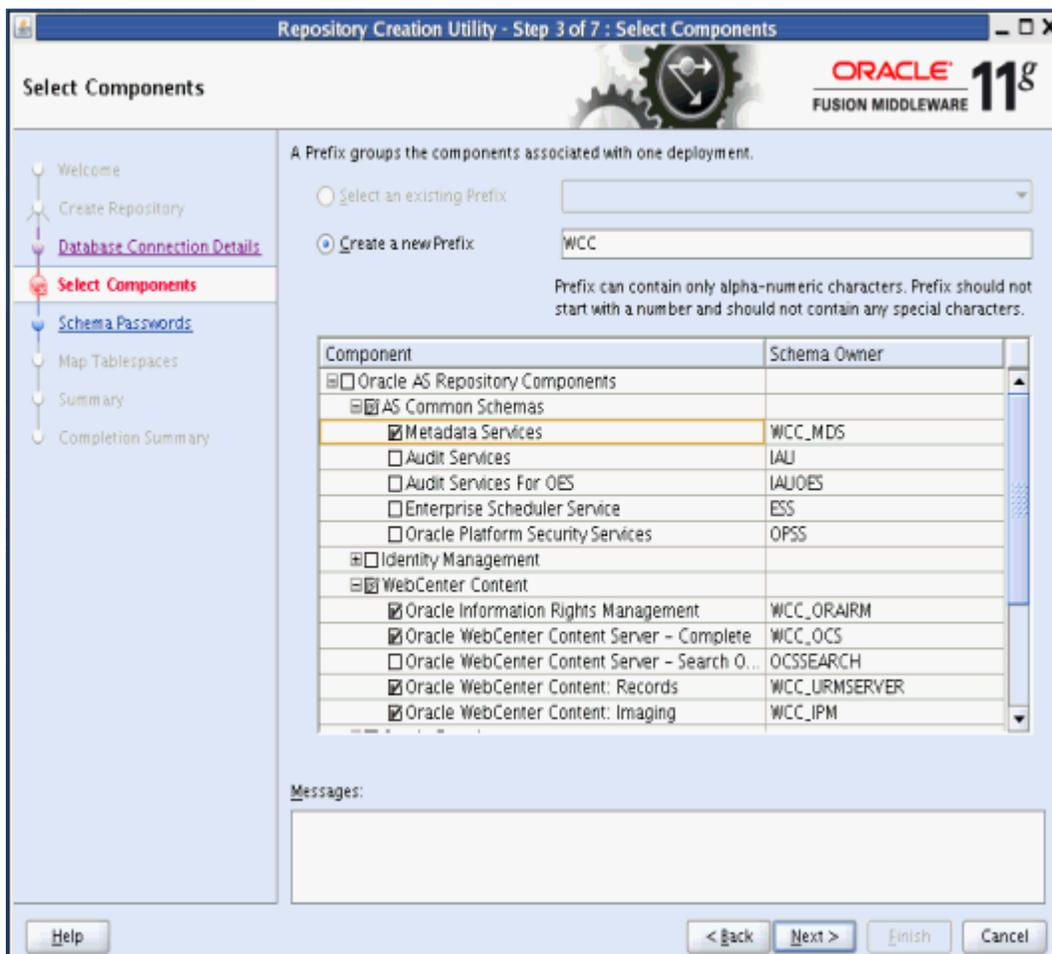
Near the top of the screen, select **Create a new Prefix**, and specify a prefix, or leave the default prefix, DEV. The prefix identifies your schema in the database. If more than one schema for the same product is stored in the database, each schema owner needs to specify a unique prefix.

For Oracle Database or Microsoft SQL Server, the prefix can contain from 1 to 12 alphanumeric characters (0-9, a-z, or A-Z).

For IBM DB2, the prefix can contain only 4 characters because the entire schema owner name is limited to 8 characters. 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_. If the default name of the schema suffix is longer than 3 characters, you need to change it for IBM DB2. For example, DEV_URMSERVER could be DEV_URM and DEV_ORAIRM could be DEV_IRM.

Expand **WebCenter Content** (for Oracle WebCenter Content applications) in the **Component** column, and select one or more of the following applications:

- **Oracle Information Rights Management**

- **Oracle WebCenter Content Server - Complete**

  (for WebCenter Content)

- **Oracle WebCenter Content Server - Search Only**

- **Oracle WebCenter Content: Records**

- **Oracle WebCenter Content: Imaging**

To create a schema for WebCenter Content, select **Oracle WebCenter Content Server - Complete**.

To create an OCSSEARCH schema for OracleTextSearch for an external data source or for IBM DB2 database searches, select **Oracle WebCenter Content Server - Search Only**. For more information, see Section 4.3.2, "Configuring the Content Server Instance," and Section 4.4, "Configuring OracleTextSearch for Content Server."

If you select **Oracle WebCenter Content: Imaging**, you should also select **Oracle WebCenter Content Server - Complete** to use WebCenter Content as the Imaging repository.

Also, for Oracle WSM Policy Manager or for using Imaging with Oracle SOA Suite, expand **AS Common Schemas**, and select **Metadata Services**. If you are using Microsoft SQL Server for the back-end database, you need to configure MDS as described in Step 4 before you select **Metadata Services** on this screen.

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

> **Note:** Record each schema owner 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 owner name for the Records schema in Oracle Database:
>
> `DEV_URMSERVER`
>
> For IBM DB2, however, the schema owner name is limited to 8 characters, with up to 4 characters for the prefix. If the default name of the schema suffix is longer than 3 characters, you need to change it for IBM DB2 on the Configure JDBC Component Schema screen. For example, `DEV_URMSERVER` could be `DEV_URM` and `DEV_ORAIRM` could be `DEV_IRM`.

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

   Specify a password for the schema owner.

   For Microsoft SQL Server or Oracle Database, RCU will create a new database user.

   IBM DB2 authentication uses operating system authentication, and you must create the user within the operating system running the database, using the appropriate name. The password set here must be the user's password on the database host. RCU imposes different restrictions than the operating system on the characters that you can use in the password.

   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

   The default Oracle WebCenter Content tablespaces are shown in Figure 2–2.

Figure 2–2   Default Oracle WebCenter Content Tablespaces on Map Tablespaces Screen
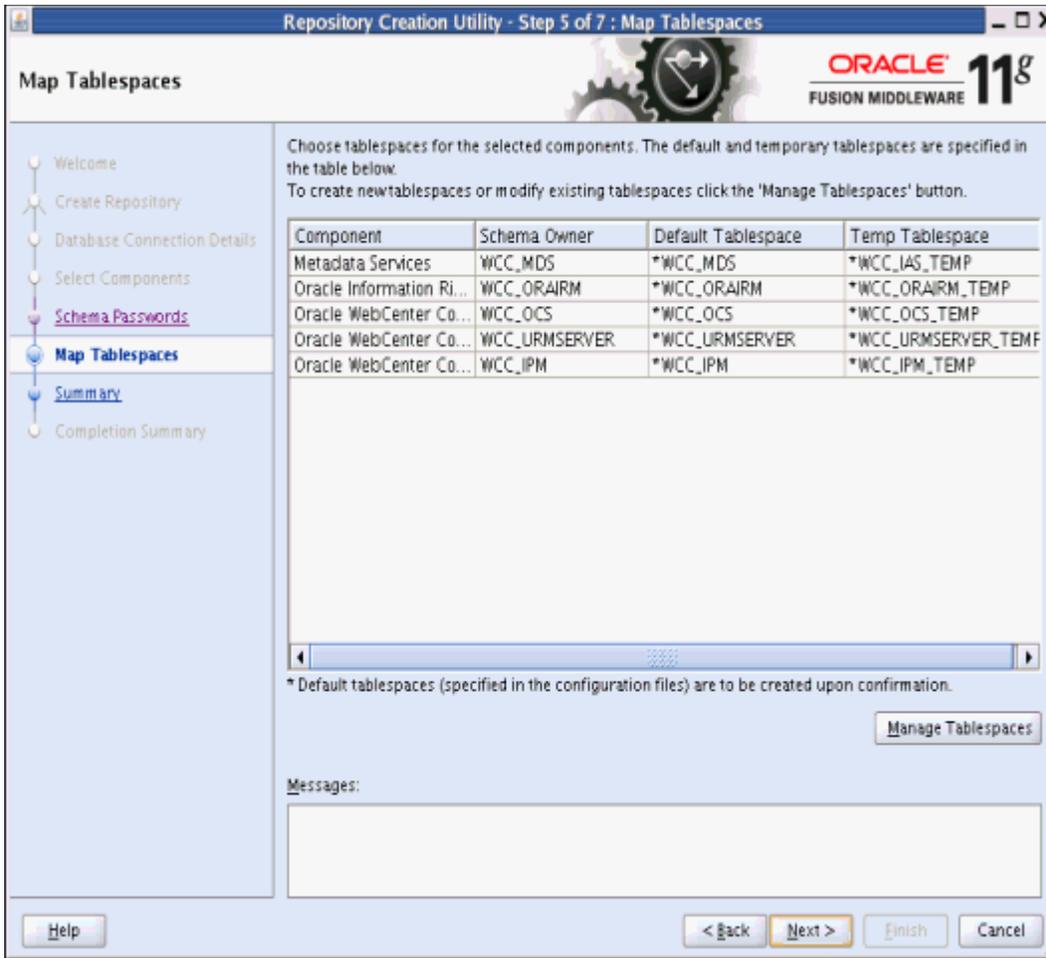
If you want to create new tablespaces or modify or remove existing ones, click **Manage Tablespaces**, and go to the next step.

To validate the tablespaces, 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.

Notes:

- For an IBM DB2 database, any tablespace that `PUBLIC` has access to is required to have a 32 KB page size. WebCenter Content requires a 32 KB page size to create tables at design time. All the tablespaces that `PUBLIC` has access to are accessible by WebCenter Content.

- If you are using an IBM DB2 database, run the following statement to prevent `PUBLIC` access to the default tablespace:

  ```
  REVOKE USE OF TABLESPACE USERSPACE1 FROM PUBLIC
  ```

  If the statement could be run multiple times, run the following statements instead:

  ```
  GRANT USE OF TABLESPACE USERSPACE1 TO PUBLIC
  REVOKE USE OF TABLESPACE USERSPACE1 FROM PUBLIC
  ```

  `Userspace1`, the default tablespace for IBM DB2, is created when a database is created. Every user has access to this tablespace. This access can cause a problem because a table created at design time, after the system is installed, could potentially put a table in this tablespace. The result would be an undesirable mix of some of an application's tables in its own tablespace and others in a tablespace that is shared by other users.

  Running the preceding `REVOKE` statement would revoke `PUBLIC` access to the default tablespace, which in turn would revoke all users' access to the tablespace. Each Oracle WebCenter Content application then would have access only to its own tablespace.

8. Manage Tablespaces screen

   On this screen, you can modify, remove, or add one or more tablespaces. Tablespaces that existed before RCU was launched are visible on this screen but are grayed out and cannot be modified or removed. Only tablespaces that are being created by RCU can be modified or removed.

   Only tablespaces that are used by a component are created. You can specify a new tablespace here, but unless it is actually used by a component, it will not be created.

   You can partition a table across tablespaces. The partitioning depends on the requirements for your installation. Typical partitioning keys are date (for example, `dInDate` in a **Revisions** table) and numeric range (such as `dID`).

   To remove a tablespace:

   a. Select the name of the tablespace you want to remove from the navigation tree on the left.

   b. Click **Remove**.

      This tablespace will not get created.

   c. Click **OK** to return to the Map Tablespaces screen, and go back to Step 7, "Map Tablespaces screen", for instructions on validating the tablespaces.

To modify or add a tablespace:

a. If you want to modify a tablespace, select the tablespace name from the navigation tree on the left.

b. If you want to add a tablespace, click **Add**.

c. Specify the values you want in these fields:

* **Name**

   Specify a name, or edit the name in this field.

* **Type**

   Specify whether you want this tablespace to be temporary or permanent.

* **Block Size (KB)**

   Specify the block size, in kilobytes, to be used for data retrieval.

* **Storage Type**

   If you want to create a tablespace for a large file or files, select **Use Bigfile Tablespace**.

   If you want to use bitmaps to manage the free space within segments, select **Use Automatic Segment Space Management**.

d. In the Datafiles section, specify the data files that make up the selected tablespace.

   To delete a data file, select the icon next to the name of the file you want to delete, then click the icon with the **X**.

   To modify a data file, select the icon next to the name of the file, and click the icon with the pencil. To add a data file, click the icon with the plus sign (+). Then, on the Add Datafile screen, edit or provide the following information:

* **File Name**

   Specify the name of the data file.

* **File Directory**

   Specify the location where this data file will reside.

* **Size**

   Specify the initial size of the data file. Use the dropdown menu next to the field to specify the size in kilobytes (**KB**), megabytes (**MB**), or gigabytes (**GB**).

* **Automatically extend datafile when full (AUTOEXTEND)**

   Select this option if you want to automatically extend the size of the data file when it becomes full.

   In the **Increment** field, specify the size by which the data file should be increased each time it becomes full. Use the dropdown menu next to the field to specify the size in kilobytes (**KB**), megabytes (**MB**), or gigabytes (**GB**).

   If you want to limit maximum size of the data file, specify this value in the **Maximum Size** field.

> **Note:** If you set the **Maximum Size** value too low, then you may have a problem when Content Server (or Records) tries to write to the database. As it reaches the size limit for the data file, the database would deny the write operation.

    e. Click **OK** to return to the Map Tablespaces screen, and go back to Step 7, "Map Tablespaces screen," for instructions on validating the tablespaces.

For more information about creating or modifying tablespaces, see "Map Tablespaces Screen" in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

9. Summary screen

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

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.

10. 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 date for an account, use the SQL statement `SELECT * FROM all_users` or `SELECT * FROM dba_users`.

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

2.3 Installing an Application Server and Oracle Fusion Middleware

Oracle WebCenter Content requires a Middleware home and an application server on your system. If your system does not already have an application server, you can install Oracle WebLogic Server with oracle Fusion Middleware in a new Middleware home directory, before or after installation of the database and creation of the schemas. Or you can install an IBM WebSphere application server, as described in the *Oracle Fusion Middleware Third-Party Application Server Guide*.

To install Oracle WebLogic Server in a Middleware home:

1. Download the Oracle WebLogic Server Installer from the Oracle Software Delivery Cloud or Oracle Technology Network (OTN) web site.

For information about downloading Oracle WebLogic Server, see Section 1.2.2, "Software Downloads for Oracle WebCenter Content Installation and Configuration."

The 32-bit executable files from which you can install Oracle WebLogic Server 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 supported JDK must be installed on your system before you install Oracle WebLogic Server because it is needed to run the JAR file.

On a Windows operating system, the JDK must be installed in a directory without spaces in the directory path (not underneath the `\Program Files` directory).

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. Copy the installer file to a directory in your local system, go to that directory, and run the installer locally, after considering these notes:

- Before running the installer on a UNIX operating system that is running XWindows, you need to set your system's DISPLAY environment variable to a valid X Server to redirect the display to a system with suitable graphic capabilities.

- If you installed a JDK for your system, set the JAVA_HOME environment variable to the installation location.

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

  To validate that your JAVA_HOME environment variable refers to a 64-bit JDK when you use a 32/64-bit hybrid JDK, run either of the following commands, in which *JAVA_HOME* is the value of the environment variable:

  JAVA_HOME/bin/java -version

  JAVA_HOME/bin/java -d64 -version

In the following commands, `wls103`*n* can be either `wls1035` or `wls1036`. To run the installer on a 32-bit Linux operating system, use this command:

./wls103*n*_linux32.bin

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

wls103*n*_win32.exe

To run the installer on a 64-bit UNIX operating system, use either of these commands, in which *JAVA_HOME* is the location of the JDK:

JAVA_HOME/bin/java -jar wls103*n*_generic.jar

JAVA_HOME/bin/java -d64 -jar wls103*n*_generic.jar

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

JAVA_HOME\bin\java -jar wls103*n*_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 WebCenter Content.

The default Oracle Middleware home is `user_home/Oracle/Middleware` on a UNIX operating system or `user_home\Oracle\Middleware` on a Windows operating system. For more information, see "Middleware Home and WebLogic Server Home Directories" in the *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** to install Oracle WebLogic Server, Oracle Coherence, and the Sun and JRockit JDKs.

Click **Next**.

If you are prompted for a JDK location on a 64-bit system, specify a JDK:

a. Browse to the JDK location.

b. Select the directory that contains the bin directory

c. 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 in this document. The default location for `WL_HOME` follows:

- **UNIX path:** `MW_HOME/wlserver_10.3`

- **Windows path:** `MW_HOME\wlserver_10.3`

You can also change the installation directory for Oracle Coherence. The default location follows:

- **UNIX path:** `MW_HOME/coherence_3.7`

- **Windows path:** `MW_HOME\coherence_3.7`

For more information about home directories, see "Middleware Home and WebLogic Server Home Directories" in the *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 operating 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 the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

2.4 Using the Installer for Oracle WebCenter Content

You can install Oracle WebCenter Content before or after you create schemas for the Oracle WebCenter Content applications. When you use the Oracle Fusion Middleware 11*g* WebCenter Content Installer, you perform a base installation of the following products in a WebCenter Content Oracle home directory on your system:

- Oracle WebCenter Content (WebCenter Content, which includes Oracle WebCenter Content Server)

- Oracle WebCenter Content: Inbound Refinery (Inbound Refinery)

- Oracle WebCenter Content: Imaging (Imaging)

- Oracle Information Rights Management (Oracle IRM)

- Oracle WebCenter Content: Records (Records)

After you install Oracle WebCenter Content and create application schemas, you can deploy any of these products to an Oracle WebLogic Server domain, as applications, by creating or extending an Oracle WebLogic Server domain. For information about application schemas, see Section 2.2, "Creating Oracle WebCenter Content Schemas with the Repository Creation Utility."

> **Note:** For document conversions on a Solaris SPARC platform,
> Imaging 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
> Imaging. 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
> Imaging Managed Server. If you are using a later version of GCC, set
> that version instead of `3.4.2`.

2.4.1 Starting the Installer

You can start the Oracle Fusion Middleware 11*g* WebCenter Content Installer from
Disk 1 of the media:

- **UNIX command:**
  wc_content_media_loc/Disk1/runInstaller -jreLoc *jre_location*

  If you do not specify the JRE location, the installer either prompts you for the
  location or returns an error. If you get an error, retry the command with the JRE
  location included.

- **Windows command:**
  wc_content_installer_loc/Disk1/setup.exe -jreLoc *jre_location*

  If you double-click setup.exe, the installer either prompts you for the JRE
  location or returns an error. If you get an error, enter the command with the JRE
  location included. If you are prompted for the JRE location, enter the path, and
  then click **Enter** to start the Oracle WebCenter Content installation.

The installer requires the location of a Java Runtime Environment (JRE) on your
system. A JRE was installed with Oracle Fusion Middleware. Table 2–1 shows the
default JRE locations.

Table 2–1   Default JRE Locations

Operating System	Production Environment	Development Environment
UNIX	*MW_HOME*/jrockit_160_29_*string*/jre	*MW_HOME*/jdk160_29/jre
Windows	*MW_HOME*\jrockit_160_29_*string*\jre	*MW_HOME*\jdk160_29\jre

You can either use the `-jreLoc` option or allow the installer to prompt for the
directory containing the `bin/java` directory

> **Notes:**
>
> - Running the installer as the user `root` is not supported.
>
> - When you start the Oracle Fusion Middleware 11*g* WebCenter Content Installer on WebSphere Application Server, you must specify the `-jreLoc` option. For more information, see "Special Instructions When Installing Oracle Fusion Middleware with IBM WebSphere" in the *Oracle Fusion Middleware Third-Party Application Server Guide*.
>
> - For the IBM JDK with Oracle WebCenter Content and WebSphere Application Server, certain functionality, such as the check for patches feature, will not work correctly unless the Java socket factories are changed. The IBM JRE has its own Secure Sockets Layer (SSL) socket factories. For more information, see "Changing Java Socket Factories in the IBM JDK" in the *Oracle Fusion Middleware Third-Party Application Server Guide*.

2.4.2 Following the Installation Instructions

After you have started the installer, as described in Section 2.4.1, follow the instructions in Table 2–2 to install Oracle WebCenter Content.

If you need additional help with any of the installation screens, see Appendix A, "Installation Screens for Oracle WebCenter Content," or click **Help** on a screen to access the online help.

Table 2–2   Installation Procedure for Oracle WebCenter Content

Screen	When This Screen Appears	Description and Action to Take
Welcome	Always	Click **Next** to begin the installation process.
Install Software Updates	Always	Specify any software updates to install before you install Oracle WebCenter Content.
		To get updates from My Oracle Support (formerly Oracle*MetaLink*), you can select **Search My Oracle Support for Updates**, specify a user name and password, and then click **Search for Updates**. Before you search, you can click **Proxy Settings** to change the settings for the proxy server and **Test Connection** to test the credentials.
		To get updates that you have saved to your computer, you can select **Search Local Directory for Updates**, specify a directory, and then click **Search for Updates**.
		If you do not want to update any software, select **Skip Software Updates**, and then click **Next** to continue the installation.
Prerequisite Checks	Always	If the installer displays an error message in the bottom section of the screen, fix the error, and then click **Retry** to start the prerequisite checking again for all applications. Repeat this until the prerequisite checks complete with no errors.
		If you want to stop the installation process while you fix a prerequisite error, click **Abort**.
		If you want to continue the installation without fixing an error, click **Continue**.
		After the prerequisite checks complete with no errors, click **Next** to continue the installation.

Table 2–2   (Cont.) Installation Procedure for Oracle WebCenter Content

Screen	When This Screen Appears	Description and Action to Take
Specify Installation Location	Always	Specify the Middleware home (*MW_HOME*) and WebCenter Content Oracle home (*WC_CONTENT_ORACLE_HOME*) locations.
		Enter values into the following fields:
		■ **Oracle Middleware Home:** Select the Middleware home directory (*MW_HOME*, which was created during the installation of Oracle WebLogic Server.
		The default Oracle Middleware home is *user_home*/Oracle/Middleware on a UNIX operating system or *user_home*\Oracle\Middleware on a Windows operating system.
		■ **Oracle Home Directory:** Specify the directory where you want to install Oracle WebCenter Content.
		For Oracle WebLogic Server, 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 WebCenter Content Oracle home, represented by *WC_CONTENT_ORACLE_HOME* in path names. Runtime components cannot write to this directory. The default WebCenter Content Oracle home is MW_HOME/Oracle_ECM1 on a UNIX operating system or MW_HOME\Oracle_ECM1 on a Windows operating system.
		Note: This document refers to this directory as the WebCenter Content 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 Directories" in the *Oracle Fusion Middleware Installation Planning Guide*
		Click **Next** to continue.
Application Server	Always	Select **WebLogic Server** to install Oracle WebCenter Content on an Oracle WebLogic Server.
		Select **WebSphere Server** to install Oracle WebCenter Content on an IBM WebSphere Application Server. For more information about the rest of the installation on this application server, see "Installing and Configuring Oracle Fusion Middleware on IBM WebSphere" and "Managing Oracle WebCenter Content on IBM WebSphere Application Servers" in the *Oracle Fusion Middleware Third-Party Application Server Guide*.

Table 2–2   (Cont.) Installation Procedure for Oracle WebCenter Content

Screen	When This Screen Appears	Description and Action to Take
Installation Summary	Always	Verify the information on this screen. If you want to change the configuration, you can return to a previous screen by clicking a link in the navigation tree on the left or by clicking **Back** until you get to the screen. After you edit the configuration, you can continue the installation from the previous screen.
		Click **Save** if you want to save a response file. You will be prompted for a name and location for the response file, which will contain information specific to your installation. After the installer creates the response file, you can use it exactly as is to replicate the installation on other systems, or you can modify the response file in a text editor.
		Click **Install** to start the software installation.
Installation Progress	Always	Monitor the progress of your installation.
		If the installer prompts you to go to `Disk 2`, specify the location of `Disk 2`, and click **OK** to resume the installation.
		If you want to stop the installation, click **Cancel**.
		After the progress reaches 100%, click **Next** to go to the last screen.
Installation Complete	Always	Click **Save** to save the installation configuration, and then click **Finish** to exit the installer.

2.5 Verifying the Installation

After you complete the installation, you can verify it by checking the log file and the directory structure.

2.5.1 Viewing the Installation Log File

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

- **UNIX location:** *USER_HOME*/oraInventory/logs/install*date_time*

- **Windows location:** *USER_HOME*\oraInventory\logs\install*date_time*

2.5.2 Checking the Directory Structure

After installation, you can verify that the directory structure is like the topology that Figure 1–3 shows.

3

Configuring Oracle WebCenter Content Applications

This chapter explains how to configure Oracle WebCenter Content applications in an Oracle WebLogic Server domain.

This chapter includes the following sections:

3.1 Preparing to Configure Oracle WebCenter Content Applications

After you have successfully run the Oracle Fusion Middleware 11*g* Oracle WebCenter Content Installer and created application schemas, you can deploy and configure the following Oracle WebCenter Content products as applications:

- Oracle WebCenter Content (which includes Oracle WebCenter Content Server)

- Oracle WebCenter Content: Inbound Refinery

- Oracle WebCenter Content: Imaging

- Oracle Information Rights Management

- Oracle WebCenter Content: Records

To configure any of these applications, you need to 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.

> **Notes:**
>
> - For information about application schemas, see Section 2.2, "Creating Oracle WebCenter Content Schemas with the Repository Creation Utility."
>
> - Each of these applications needs to run in its own Managed Server or its own cluster of Managed Servers. You cannot deploy WebCenter Content, Inbound Refinery, Imaging, Oracle IRM, or Records to a Managed Server or cluster that already has another application deployed. Oracle WebCenter Content applications should not be deployed to the Administration Server.
>
> - Only one Managed Server for each of the Oracle WebCenter Content applications, such as WebCenter Content, can be configured in the same Oracle Weblogic Server domain. If you want to put multiple WebCenter Content Managed Servers on the same machine, you need to configure each Managed Server in a separate domain.
>
> - If you are using a DB2 database, before you start the Configuration Wizard for the first time to configure an Oracle Fusion Middleware product, you need to set the *DB_DRIVER_ CLASSPATH* environment variable to include the full paths to db2jcc4.jar and db2jcc_license_cu.jar. If you do not do this, all DB2 connection tests will fail.

You can create a domain to include one or more of these applications (one Managed Server each). Or you can create a domain to include a Managed Server for at least one application and then extend the domain with Managed Servers for one or more other applications.

> **Note:** WebCenter Content cannot be deployed to the same domain as Oracle Identity Manager and Oracle Identity Management.

On a Windows operating system, you can run Oracle WebCenter Content Managed Servers as services.

For Imaging to take advantage of Business Process Management (BPM) and Oracle BPEL Process Manager within an existing domain, the domain must be extended with Oracle BPM Suite. If you want to use Oracle BPEL Process Manager and not BPM, you can extend the domain with Oracle SOA Suite. For information about connecting to BPM or Oracle BPEL Process Manager as a workflow server, see "Creating a Workflow Connection" in the *Oracle WebCenter Content Administrator's Guide for Imaging*.

> **Note:** The Imaging 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 2, "Installing Oracle WebCenter Content."

To create a domain for one or more Oracle WebCenter Content applications, follow the instructions in Section 3.2, "Creating an Oracle WebLogic Server Domain."

To extend an existing domain for one or more Oracle WebCenter Content applications, follow the instructions in Section 3.3, "Extending an Existing Domain."

> **Note:** You cannot extend a domain that has an Oracle WebCenter Content 11.1.1.2.1 or 11.1.1.3.0 application to include an Oracle WebCenter Content 11.1.1.6.0 application.

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, "Configuration Screens for Oracle WebCenter Content," 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 Fusion Middleware Control for administration of Oracle WebCenter Content 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.

For information about configuring Fusion Middleware Control for Oracle WebCenter Content on an IBM WebSphere Application Server, see "Using Oracle Enterprise Manager Fusion Middleware Control" in the *Oracle Fusion Middleware Third-Party Application Server Guide*.

3.2 Creating an Oracle WebLogic Server Domain

You can create an Oracle WebLogic Server domain for Oracle WebCenter Content with Fusion Middleware Configuration Wizard. When you create a domain for Oracle WebCenter Content, you configure one or more of its applications.

The configuration wizard is in the following directory. *WC_CONTENT_ORACLE_HOME* represents the WebCenter Content Oracle home directory, where Oracle WebCenter Content is installed:

- **UNIX path:** *WC_CONTENT_ORACLE_HOME*/common/bin

- **Windows path:** *WC_CONTENT_ORACLE_HOME*\common\bin

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

- **UNIX script:**
  WC_CONTENT_ORACLE_HOME/common/bin/config.sh -log=*log_file_name*

  Your log file will be created in your *oraInventory_location/logs /installActions*/logs directory.

- **Windows script:**
  WC_CONTENT_ORACLE_HOME\common\bin\config.cmd -log=*log_file_name*

  Your log file will be created in your *inventory_location*\logs\installActions\logs directory. The default *inventory_location* value follows:

  ```
  %PROGRAMFILES%\Oracle\Inventory
  ```

Table 3–1 describes the steps for creating a domain and provides some links to screen descriptions in Appendix B, "Configuration Screens for Oracle WebCenter Content."

Table 3–1   Procedure for Creating a New Domain

Screen	When This Screen Appears	Description and Action to Take
None		Start Fusion Middleware Configuration Wizard:
		■ **UNIX script:** *WC_CONTENT_ORACLE_HOME*/common/bin /config.sh[-log=*log_file_name*]
		■ **Windows script:** *WC_CONTENT_ORACLE_HOME*\common\bin \config.cmd[-log=*log_file_name*]
Welcome	Always	Select **Create a new WebLogic Domain**.
		Click **Next** to continue.
Select Domain Source	Always	Select **Generate a domain configured automatically to support the following products**, and then select one or more of these templates:
		■ **Oracle WebCenter Content: Imaging**
		■ **Oracle Universal Records Management**
		(for Oracle WebCenter Content: Records)
		■ **Oracle Universal Content Management - Inbound Refinery**
		(for Oracle WebCenter Content: Inbound Refinery)
		■ **Oracle Universal Content Management - Content Server**
		(for Oracle WebCenter Content)
		■ **Oracle Information Rights Management**
		When you select **Oracle WebCenter Content: Imaging**, you also need to select **Oracle WebCenter Content - Content Server**, if WebCenter Content is not already configured.
		When you select any Oracle WebCenter Content application on the Select Domain Source screen, **Oracle Enterprise Manager** and **Oracle JRF** are automatically selected. If you deselect any of these items that are automatically selected, the Oracle WebCenter Content application will also be deselected.
		If you want a remote deployment of a Site Studio for External Applications web site, you can select **Oracle Universal Content Management - SSXA Server** (for Oracle WebCenter Content - SSXA Server) to create an Oracle WebLogic Server domain with a Managed Server that has the files required to run the web site.
		To create a domain that includes Oracle Web Services Manager (Oracle WSM) Policy Manager, select **Oracle WSM Policy Manager**.
		Click **Next** to continue.

Table 3–1   (Cont.) Procedure for Creating a New Domain

Screen	When This Screen Appears	Description and Action to Take
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 follows (*MW_HOME* represents the Middleware home directory):
		■ **UNIX path:** *MW_HOME*/user_projects/domains
		■ **Windows path:** *MW_HOME*\user_projects\domains
		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 WebCenter Content application in the **Application location** field. The default location is *MW_HOME*/user_projects/applications/.
		Click **Next** to continue.
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 Managed Servers and to access the domain through the Oracle WebLogic Server Administration Console or Fusion Middleware Control.
		Click **Next** to continue.
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 1.6.0_29**, and the default JDK for production mode is **JRockit SDK 1.6.0_29**, except on a 64-bit system, where the default JDK is the one you installed. To specify a different JDK, select **Other JDK**, and enter its location.
		Click **Next** to continue.

Table 3–1 (Cont.) Procedure for Creating a New Domain

Screen	When This Screen Appears	Description and Action to Take
Configure JDBC Component Schema	Always	Configure each component schema, including the Oracle WSM MDS schema if it was created with Repository Creation Utility (RCU), by selecting a schema checkbox and then completing 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 or IBM DB2, 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 is 1521 for an Oracle Database instance, `1433` for Microsoft SQL Server, or `50000` for IBM DB2.
		Click **Next** to continue.
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.

Table 3–1 (Cont.) Procedure for Creating a New Domain

Screen	When This Screen Appears	Description and Action to Take
Select Optional Configuration	Always	Optionally, select any or all of these options for configuring the Administration Server and Managed Servers:
		■ **Administration Server**
		■ **JMS Distributed Destination**
		■ **Managed Servers, Clusters and Machines**
		■ **Deployments and Services**
		■ **RDBMS Security Store**
		Select one or more of these options if you want to change any default settings. For example, select **Administration Server** to configure SSL for it or change its port number, or select **Managed Servers, Clusters and Machines** to change the name or port for a Managed Server, add it to a cluster, or configure a machine for it.
		For Oracle IRM, you should select **Administration Server**, **Managed Servers, Clusters and Machines**, and **Deployments and Services**.
		Note: To use clusters, you need a license for Oracle WebLogic Server Enterprise Edition.
		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.
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.
		Note: If SSL is enabled, before you use WLST to connect to the Administration Server, you must either append the following parameters to the JVM_ARGS section of the wlst.sh file or set them in the CONFIG_JVM_ARGS environment variable:
		`-Dweblogic.security.SSL.ignoreHostnameVerification=true`
		`-Dweblogic.security.TrustKeyStore=KeyStoreName`
		`KeyStoreName` is the name of the keystore in use (`DemoTrust` for the built-in demonstration certificate). The wlst.sh file is in the bin subdirectory of the common directory in the WebCenter Content Oracle home directory.
		Click **Next** to continue.
Select JMS Distributed Destination Type	If you selected Oracle Imaging and Process Management (for Oracle WebCenter Content: Imaging) on the Select Domain Source screen.	Accept the default (UDD), and click **Next**. Click **OK** in the override warning.

Table 3–1   (Cont.) Procedure for Creating a New Domain

Screen	When This Screen Appears	Description and Action to Take
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 3–2 lists the default port values for the Managed Servers that run Oracle WebCenter Content 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 configured so that Content application server 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 Rights Desktop.
		Click **Next** to continue.
Configure Clusters	If you selected **Managed Servers, Clusters and Machines** on the Select Optional Configuration screen.	Optionally, configure one or more clusters.
		Notes:
		■ To use clusters, you need a license for Oracle WebLogic Server Enterprise Edition.
		■ If you decide to configure a cluster, then you must assign a cluster address.
		Click **Next** to continue.
Assign Servers to Clusters	If you configured any clusters on the Configure Clusters screen	Assign two or more of the Managed Servers in the domain to each cluster.
		Click **Next** to continue.
Create HTTP Proxy Applications	If you configured any clusters on the Configure Clusters screen and assigned some, but not all, of the Managed Servers in the domain to a cluster	Create a proxy application for each Managed Server that you did not assign to a cluster in the domain.
		Click **Next** to continue.
Configure Machines	If you selected **Managed Servers, Clusters and Machines** on the Select Optional Configuration screen.	Optionally, configure machines to host Managed Servers, and assign a Managed Server to each machine.
		Click **Next** to continue.
Assign Servers to Machines	If you added any machines on the Configure Machines screen	Assign at least one server to each machine.
		Click **Next** to continue.

Table 3–1   (Cont.) Procedure for Creating a New Domain

Screen	When This Screen Appears	Description and Action to Take
Target Deployments to Clusters or Servers	If you selected **Deployments and Services** on the Select Optional Configuration screen.	Optionally, assign each application to the Administration Server, a Managed Server, or a cluster of Managed Servers.
		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` value will be replicated. Otherwise, `memory` is the default.
		When deploying Oracle IRM to a cluster, make sure that the Oracle IRM application is deployed to all nodes.
		Click **Next** to continue.
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.
		Click **Next** to continue.
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.
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.
Creating Domain	Always	On a Windows operating system, you can select **Start Admin Server** to start the Administration Server as soon as the configuration is done.
		When the domain is created successfully, click **Done**.

Table 3–2 lists the default port values for the Managed Servers that run Oracle WebCenter Content applications.

Table 3–2   Default Ports for Managed Servers

Managed Server	Default Listen Port	Default SSL Port	Port Range
Imaging	16000	16001	16000–16099
Oracle IRM	16100	16101	16100–16199
WebCenter Content	16200	16201	16200–16299
Inbound Refinery	16250	16251	16200–16299
Records	16300	16301	16300–16399

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. Before you start a Managed Server, see the rest of the configuration information in this chapter and in the configuration chapter for your application. For more information, see Section 9.2, "Starting Managed Servers."

3.3 Extending an Existing Domain

You can extend an existing Oracle WebLogic Server domain to configure one or more Oracle WebCenter Content applications. Fusion Middleware Configuration Wizard is in the following directory:

- **UNIX path:** *WC_CONTENT_ORACLE_HOME*/common/bin

- **Windows path:** *WC_CONTENT_ORACLE_HOME*\common\bin

Notes:

- WebCenter Content cannot be deployed to the same domain as Oracle Identity Manager and Oracle Identity Management.

- You cannot extend a domain that has an Oracle Enterprise Content Management Suite application from an earlier release to include an Oracle WebCenter Content 11.1.1.6.0 application.

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 a Oracle IRM Managed Server. Or you could extend an Imaging 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 3–3 describes the steps for extending a domain and provides some links to screen descriptions in Appendix B, "Configuration Screens for Oracle WebCenter Content."

Table 3–3   Procedure for Extending an Existing Domain

Screen	When This Screen Appears	Description and Action to Take
None.	Always	Start Fusion Middleware Configuration Wizard: ■ **UNIX script:** *WC_CONTENT_ORACLE_HOME*/common/bin/config.sh [-log=*log_file_name*] ■ **Windows script:** *WC_CONTENT_ORACLE_HOME*\common\bin\config.cmd [-log=*log_file_name*]
Welcome	Always	Select **Extend an existing WebLogic Domain**. Click **Next** to continue.
Select a WebLogic Domain Directory	Always	Select a directory for adding your applications or services, or both. Click **Next** to continue.
Select Extension Source	Always	Select **Extend my domain automatically to support the following added products**, and then select one or more of these templates: ■ **Oracle WebCenter Content: Imaging** ■ **Oracle Universal Records Management** (for Oracle WebCenter Content: Records) ■ **Oracle Universal Content Management - Inbound Refinery** (for Oracle WebCenter Content: Inbound Refinery) ■ **Oracle Universal Content Management - Content Server** (for Oracle WebCenter Content) ■ **Oracle Information Rights Management** When you select **Oracle WebCenter Content: Imaging**, you also need to select **Oracle WebCenter Content - Content Server**, if WebCenter Content is not already configured. When you select any Oracle WebCenter Content application on the Select Extension Source screen, **Oracle Enterprise Manager** and **Oracle JRF** are automatically selected. If you deselect any of these items that are automatically selected, the Oracle WebCenter Content application will also be deselected. If you want a remote deployment of a Site Studio for External Applications web site, you can select **Oracle Universal Content Management - SSXA Server** (for Oracle WebCenter Content - SSXA Server) to extend an Oracle WebLogic Server domain with a Managed Server that has the files required to run the web site. To extend a domain that includes Oracle Web Services Manager (Oracle WSM) Policy Manager, select **Oracle WSM Policy Manager**. Click **Next** to continue.

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

Screen	When This Screen Appears	Description and Action to Take
Configure JDBC Component Schema	Always	Configure each component schema, including the Oracle WSM 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 is 1521 for an Oracle Database instance, `1433` for Microsoft SQL Server, or `50000` for IBM DB2.
		Click **Next** to continue.
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.

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

Screen	When This Screen Appears	Description and Action to Take
Select Optional Configuration	Always	Optionally, select any or all of these options for configuring Managed Servers:
		■ **JMS Distributed Destination**
		■ **Managed Servers, Clusters and Machines**
		■ **Deployments and Services**
		■ **RDBMS Security Store**
		Select one or more of these options if you want to change any default settings. For example, select **Administration Server** to configure SSL for it or change its port number, or select **Managed Servers, Clusters and Machines** to change the name or port for a Managed Server, add it to a cluster, or configure a machine for it.
		Note: To use clusters, you need a license for Oracle WebLogic Server Enterprise Edition.
		For Oracle IRM, you should select **Administration Server**, **Managed Servers, Clusters and Machines**, and **Deployments and Services**.
		If you are extending a domain that already includes WebCenter Content with Imaging and plan to use WebCenter Content 11*g* as the Imaging repository, select **Managed Servers, Clusters and Machines** so you can configure a separate machine for running the Imaging Managed Server.
		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.
Select JMS Distributed Destination Type	If you selected Oracle Imaging and Process Management (for Oracle WebCenter Content: Imaging) on the Select Extension Source screen.	Accept the default (UDD), and click **Next**. Click **OK** in the override warning.
[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 3–2 lists the default port values for the Managed Servers that run Oracle WebCenter Content 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 configured so that Rights 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 Rights Desktop.
		Click **Next** to continue.

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

Screen	When This Screen Appears	Description and Action to Take
Configure Clusters	If you selected **Managed Servers, Clusters and Machines** on the Select Optional Configuration screen.	Optionally, change the cluster configuration. **Notes:** ▪ To use clusters, you need a license for Oracle WebLogic Server Enterprise Edition. ▪ If you decide to configure a cluster, then you must assign a cluster address. You need an Oracle WebLogic Server Enterprise Edition license to use clusters. Click **Next** to continue.
Assign Servers to Clusters	If you configured any clusters on the Configure Clusters screen	Assign two or more of the Managed Servers in the domain to each cluster. Click **Next** to continue.
Create HTTP Proxy Applications	If you configured any clusters on the Configure Clusters screen and assigned some, but not all, of the Managed Servers in the domain to a cluster	Create a proxy application for each Managed Server in the domain that you did not assign to a cluster. Click **Next** to continue.
Configure Machines	If you selected **Managed Servers, Clusters and Machines** on the Select Optional Configuration screen.	Optionally, configure machines to host Managed Servers, and assign a Managed Server to each machine. If you are extending a domain that already includes WebCenter Content with Imaging and plan to use WebCenter Content 11*g* as the Imaging repository, configure a separate machine and assign the Imaging Managed Server to it. Click **Next** to continue.
Assign Servers to Machines	If you added any machines on the Configure Machines screen	Assign at least one server to each machine. Click **Next** to continue.
Target Deployments to Clusters or Servers	If you selected **Managed Servers, Clusters and Machines** on the Select Optional Configuration screen.	Optionally, assign each application to the Administration Server, a Managed Server, or a cluster of Managed Servers. 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` value 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.

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

Screen	When This Screen Appears	Description and Action to Take
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. Click **Next** to continue.
Configuration Summary	Always.	When the configuration is satisfactory, click **Extend** to extend the domain.
Creating Domain	Always	On a Windows operating system, you can select **Start Admin Server** to start the Administration Server as soon as the configuration is done. 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. Before you start a Managed Server, see the rest of the configuration information in this chapter and in the configuration chapter for your application. For more information, see Section 9.2, "Starting Managed Servers."

3.4 Extending a Domain in an SSL Environment

If your Oracle WebLogic Server domain connects to a database through an SSL port, you need to back up your data source and SSL parameters and remove the SSL configuration from the data source before running Fusion Middleware Configuration Wizard to extend the domain. After you have successfully extended the domain, you can restore the SSL configuration to your data source.

To extend a domain in an SSL environment with Fusion Middleware Configuration Wizard:

1. In the Oracle WebLogic Server Administration Console, select your data source, and save a backup of all SSL parameters.

    Back up the URL, `javax.net.ssl.trustStorePassword`, `javax.net.ssl.trustStore`, `javax.net.ssl.trustStoreType`, and any other SSL parameters that have been configured for the data source.

2. Temporarily replace the SSL configuration for the data source with a non-SSL configuration.

Use a non-SSL URL and remove all SSL properties. You should end with something like this configuration:

- URL:

  ```
  :  jdbc:oracle:thin:@myhost.example.com:1521:db11107
  ```

- Properties:

  - ```
    user=MAR20SSL_OCS
    ```

  - ```
    oracle.net.CONNECT_TIMEOUT=10000
    ```

  - ```
    sendStreamAsBlob=true
    ```

3. Using Fusion Middleware Configuration Wizard, extend the domain, as described in Table 3–3.

4. After successfully extending the domain, restore the SSL configuration to your data source. You should end with something like this configuration:

- URL:

  ```
  jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_
  LIST=(ADDRESS=(PROTOCOL=TCPS)(HOST=myhost.example.com)(PORT=2490)))(CONNECT
  _DATA=(SERVICE_NAME=db11107.example.com))(SECURITY=(SSL_SERVER_CERT_
  DN="CN=myhost.example.com,OU=QA,O=ECM,L=RedwoodShores,ST=California,C=US"))
  )
  ```

- Properties:

  - ```
    javax.net.ssl.trustStorePassword=DemoTrustKeyStorePassPhr
    ase
    ```

  - ```
    user=MAR20SSL_OCS
    ```

  - ```
    javax.net.ssl.trustStore=/mw_home/wlserver_
    10.3/server/lib/DemoTrust.jks
    ```

  - ```
    oracle.net.CONNECT_TIMEOUT=10000
    ```

  - ```
    javax.net.ssl.trustStoreType=JKS
    ```

  - ```
    javax.net.ssl.trustStoreType=JKS
    ```

  - ```
    sendStreamAsBlob=true
    ```

5. If during step 3 you updated your domain with a new product that creates its own data source, you may need to add SSL configuration to it as well.

3.5 Increasing the Java VM Heap Size for Managed Servers

You need to increase the size of the heap allocated for the Java Virtual Machine (VM) on which each Managed Server runs to at least 1 GB (1024 MB). If you do not increase the Java VM heap size, then Oracle support and development will not accept any escalation of runtime issues, especially out-of-memory issues.

For a Managed Server using the Sun JDK, you need to set the size of the heap allocated for the Java VM to 512 MB rather than 1 GB so that programs configured to use all available space will not fail at initialization. Address space must be reserved for permanent objects, and the `MaxPermSize` setting for each Managed Server reduces the space available for the rest of the heap.

There are two common ways to adjust the runtime memory parameters for a Managed Server:

- Setting Server Startup Parameters for Managed Servers with the Administration Console

  This method is required if the Managed Server process will be run from Node Manager. For more information about running Managed Servers from Node Manager, see Section 9.4, "Using Node Manager with Oracle WebCenter Content."

- Setting the USER_MEM_ARGS Environment Variable for a Managed Server

  This method is required if the managed server process will be run directly from the command line. For more information about running Managed Servers from the command line, see Section 9.2, "Starting Managed Servers."

3.5.1 Setting Server Startup Parameters for Managed Servers with the Administration Console

You can set server startup parameters with the Oracle WebLogic Server Administration Console. This is the preferred approach for setting startup parameters because it ensures that the parameters are correctly pushed to each server, and it avoids problems that might occur during manual editing of server startup scripts. To increase the Java VM heap size, you set the value of the `-Xmx` parameter.

To set server startup parameters for Managed Servers with the Administration Console:

1. Log in to the Oracle WebLogic Server Administration Console 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.example.com: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.

2. Click **Environment** under Domain Structure, on the left.

3. Click **Servers** on the Summary of Environment page.

4. Set the memory parameters for each Managed Server:

   a. Click the name of a Managed Server in the Servers table.

   b. On the **Configuration** tab, in the second row of tabs, click **Server Start**.

   c. In the **Arguments** box, paste a string that specifies the memory parameters.

   Table 3–4 shows parameters to specify for Sun and JRockit Java VMs on UNIX and Windows operating systems. Other Java VMs may have different values.

Table 3–4   Java VM Memory Parameters

Java VM	Operating System	Parameters
Sun	UNIX	`-Xms256m -Xmx1024m -XX:CompileThreshold=8000 -XX:PermSize=128m -XX:MaxPermSize=512m`
Sun	Windows	`-Xms256m -Xmx1024m -XX:CompileThreshold=8000 -XX:PermSize=128m -XX:MaxPermSize=512m`
JRockit	UNIX	`-Xms256m -Xmx1024m -XnoOpt`
JRockit	Windows	`-Xms256m -Xmx1024m -XnoOpt`

    d. Save the configuration changes.

5. Restart any running Managed Servers, as described in Section 9.3, "Restarting a Managed Server."

3.5.2 Setting the USER_MEM_ARGS Environment Variable for a Managed Server

You can set server startup parameter for a Managed Server by setting the USER_ MEM_ARGS environment variable in its startup script or command file. To increase the Java VM heap size, you set the value of the `-Xmx` parameter.

To set the USER_MEM_ARGS Environment Variable for a Managed Server:

- UNIX shell script (`.sh`) entry

```
export USER_MEM_ARGS="-Xms256m -Xmx1024m -XX:CompileThreshold=8000
-XX:PermSize=128m -XX:MaxPermSize=512m"
```

- UNIX C shell script (`.csh`) entry

```
setenv  USER_MEM_ARGS "-Xms256m -Xmx1024m -XX:CompileThreshold=8000
-XX:PermSize=128m -XX:MaxPermSize=512m"
```

- Windows command file (`.cmd`) entry

```
set USER_MEM_ARGS="-Xms256m -Xmx1024m -XX:CompileThreshold=8000
-XX:PermSize=128m -XX:MaxPermSize=512m"
```

> **Note:** Table 3–4 shows parameters to specify for Sun and JRockit Java VMs on UNIX and Windows operating systems. Other Java VMs may have different values.

3.6 Setting Up Fonts on a UNIX System

On a UNIX operating system, you need to make sure TrueType fonts are set up for Imaging, Inbound Refinery, and WebCenter Content Dynamic Converter. If you are using a language other than English, you also need to set up fonts for national language support.

3.6.1 Setting Up TrueType Fonts on a UNIX System

For Imaging and WebCenter Content Dynamic Converter to work correctly on a UNIX operating system, you need to set up TrueType fonts on the machine where Imaging, Inbound Refinery, or the Dynamic Converter is running. If these fonts are not available on your system, you need to install them. For information about configuring

the path to the font directory for Imaging once the fonts are installed, see Section 6.1.4, "Configuring the GDFontPath MBean for a UNIX System."

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, Imaging 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 Imaging. 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 Imaging 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`
- HP-UX Itanium: `/usr/lib/X11/fonts/TrueType`
- Linux: `/usr/lib/X11/fonts/TrueType`

3.6.2 Installing Fonts for National Language Support on a UNIX System

For languages other than English, the following installation steps need to be done on a UNIX operating system before you start a Managed Server:

- Copy *MW_HOME*`/oracle_common/jdk/jre/lib/fonts` to the `/jre/lib/fonts` directory in the Sun JDK installation directory for the Middleware home.
- Copy *MW_HOME*`/oracle_common/jdk/jre/lib/fonts` to the `/jre/lib/fonts` directory in the Oracle JRockit JDK directory for the Middleware home.

3.7 Installing Libraries and Setting Environment Variables for Outside In Technology

WebCenter Content, Inbound Refinery, Imaging, and the Imaging Advanced Viewer for clients use Outside In Technology (OIT), which requires certain libraries that are not part of Oracle WebCenter Content. Before a WebCenter Content, Inbound Refinery, or Imaging Managed Server is started, you need to install the libraries for your platform. For a UNIX platform, you also need to set an environment variable to reference the libraries in the library path for the user who will start the Managed Server.

3.7.1 Installing Libraries for Outside In Technology on UNIX Platforms

Before you start a WebCenter Content, Inbound Refinery, or Imaging Managed Server, the libraries required for your platform need to be available on your system.

Many of the required libraries are normally installed on the machine, including the C, math, X11, dynamic loader, and pthreads libraries, among others. The `libgcc_s` and `libstdc++` libraries are part of the GNU Compiler Collection (GCC) package.

OIT requires the following libraries for the specified UNIX platform. The libraries in bold are part of the GCC package 3.4.2 or later.

Solaris Sparc 32-bit requires GCC package 3.4.2 or later, which you can download from the Sunfreeware web site at

http://www.sunfreeware.com

HPUX Itanium requires GCC package 3.3.6, which you can download through the following web site:

http://gcc.gnu.org

If a `libgcc_s` or `libstdc++` library is required for your platform, install the GCC package in the `/usr/local/packages/gcc-3.4.2/lib` directory in a Solaris Sparc system or the `/usr/local/packages/gcc-3.3.6/lib` or directory in an HPUX ia64 system, on the machine where Imaging or WebCenter Content will run. If you are using a later version of GCC, specify that version instead of `3.4.2` or `3.3.6`.

OIT requires the following libraries for the specified UNIX platform. The libraries in **bold** are part of the GCC package.

- Solaris Sparc 32-bit

```
/usr/platform/SUNW,Ultra-60/lib/libc_psr.so.1
libICE.so.6
libSM.so.6
libX11.so.4
libXext.so.0
libXm.so.4
libXt.so.4
libc.so.1
libdl.so.1
```
libgcc_s.so.1
```
libgen.so.1
libm.so.1
libmp.so.2
libnsl.so.1
libpthread.so.1
libsocket.so.1
```
libstdc++.so.6
```
libthread.so.1
```

- HPUX ia64

```
libCsup.so.1
libICE.so.1
libSM.so.1
libX11.so.1
libXext.so.1
libXm.so.1
libXp.so.1
libXt.so.1
libc.so.1
libdl.so.1
```
libgcc_s_hpux64.so.0
```
libm.so.1
libpthread.so.1
```

```
libstd_v2.so.1
libstdc++.so.5
libuca.so.1
libunwind.so.1
```

- AIX 32-bit

```
/usr/lib/libC.a(ansi_32.o)
/usr/lib/libC.a(shr.o)
/usr/lib/libC.a(shr2.o)
/usr/lib/libC.a(shr3.o)
/usr/lib/libICE.a(shr.o)
/usr/lib/libIM.a(shr.o)
/usr/lib/libSM.a(shr.o)
/usr/lib/libX11.a(shr4.o)
/usr/lib/libXext.a(shr.o)
/usr/lib/libXi.a(shr.o)
/usr/lib/libXm.a(shr_32.o)
/usr/lib/libXt.a(shr4.o)
/usr/lib/libc.a(shr.o)
/usr/lib/libcrypt.a(shr.o)
/usr/lib/libgaimisc.a(shr.o)
/usr/lib/libgair4.a(shr.o)
/usr/lib/libi18n.a(shr.o)
/usr/lib/libiconv.a(shr4.o)
/usr/lib/libodm.a(shr.o)
/usr/lib/libpthreads.a(shr.o)
/usr/lib/libpthreads.a(shr_comm.o)
/usr/lib/libpthreads.a(shr_xpg5.o)
/usr/lib/libpthreads_compat.a(shr.o)
```

- HPUX PA/RISC 32-bit

```
/lib/libCsup.2
/lib/libCsup_v2.2
/lib/libX11.3
/lib/libXm.4
/lib/libXt.3
/lib/libc.2
/lib/libcl.2
/lib/libm.2
/lib/libstd.2
/lib/libstd_v2.2
/lib/libstream.2
/usr/lib/libCsup.2
/usr/lib/libCsup_v2.2
/usr/lib/libX11.3
/usr/lib/libXm.4
/usr/lib/libXt.3
/usr/lib/libc.2
/usr/lib/libcl.2
/usr/lib/libdld.2
/usr/lib/libisamstub.1
/usr/lib/libm.2
/usr/lib/libstd.2
/usr/lib/libstd_v2.2
/usr/lib/libstream.2
/view/x_r6hp700_1111/vobs/swdev/pvt/r6hp700_1111/X11R6/lib/libICE.2
/view/x_r6hp700_1111/vobs/swdev/pvt/r6hp700_1111/X11R6/lib/libSM.2
/view/x_r6hp700_1111/vobs/swdev/pvt/r6hp700_1111/X11R6/lib/libX11.3
/view/x_r6hp700_1111/vobs/swdev/pvt/r6hp700_1111/X11R6/lib/libXext.3
```

```
/view/x_r6hp700_1111/vobs/swdev/pvt/r6hp700_1111/X11R6/lib/libXp.2
/view/x_r6hp700_1111/vobs/swdev/pvt/r6hp700_1111/X11R6/lib/libXt.3
```

- SUSE Linux

  For an SUSE Linux operating system, the file `/usr/lib/libstdc++.so.5` is required. You can find this file in the `compat-libstdc++` or `libstdc++33` package.

3.7.2 Setting Library Paths in Environment Variables on UNIX Platforms

Before Inbound Refinery or the WebCenter Content Dynamic Converter uses Outside In Technology for document and image conversions, the following environment variables must be set for the WebCenter Content Managed Server on the specified UNIX platforms:

- Environment variables for library paths for Imaging
  - Solaris Sparc:

    ```
    LD_LIBRARY_PATH=/usr/local/packages/gcc-3.4.2/lib:"$LD_LIBRARY_PATH"
    ```

    If you are using a later version of GCC, specify that version instead of 3.4.2.
  - AIX:

    ```
    LIBPATH=DomainHome/oracle/imaging/imaging-server
    ```

  - HP-UX Itanium:

    ```
    LD_PRELOAD=/usr/lib/hpux64/libpthread.so.1
    LD_LIBRARY_PATH=DomainHome/oracle/imaging/imaging-server:"$LD_LIBRARY_PATH"
    ```

- Environment variables for library paths for WebCenter Content with Dynamic Converter and Inbound Refinery
  - Solaris Sparc:

    ```
    LD_LIBRARY_PATH=/usr/local/packages/gcc-3.4.2/lib:"$LD_LIBRARY_PATH"
    ```

    If you are using a later version of GCC, specify that version instead of 3.4.2.

    Add the following line to the Inbound Refinery `intradoc.cfg` file at *DomainHome*/ucm/ibr/bin:

    ```
    ContentAccessExtraLibDir=/usr/local/packages/gcc-3.4.2/lib
    ```

    Then restart Inbound Refinery, as described in
  - HP-UX Itanium:

    ```
    export LD_LIBRARY_
    PATH=/opt/hp-gcc/3.3.6/lib/:/opt/hp-gcc/3.3.6/lib/hpux64:"$LD_LIBRARY_PATH"
    ```

    The Dynamic Converter on HP-UX Itanium needs the 3.3.6 version of the GCC libraries installed before the WebCenter Content server is started.

- DISPLAY environment variable

  On a UNIX operating system running XWindows, when redirecting the display to a system with suitable graphic capabilities, export DISPLAY to a valid X Server before starting the Imaging, the Inbound Refinery Managed Server, or the WebCenter Content Dynamic Converter.

3.7.3 Downloading Visual C++ Libraries for a Windows Operating System

Outside In Technology 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`.

The WinNativeConverter has some vb.Net code, so it also requires Microsoft .NET Framework 3.5 Service Pack 1.

3.8 Configuring SSL for Oracle WebCenter Content Applications

You can configure Single Sign-ON SSL for Oracle WebCenter Content applications running in a production or development environment.

> **Note:** If SSL is enabled, before you use WLST to connect to the Administration Server, you must either append the following parameters to the JVM_ARGS section of the `wlst.sh` file or set them in the CONFIG_JVM_ARGS environment variable:
>
> ```
> -Dweblogic.security.SSL.ignoreHostnameVerification=true
> -Dweblogic.security.TrustKeyStore=KeyStoreName
> ```
>
> *KeyStoreName* is the name of the keystore in use (`DemoTrust` for the built-in demonstration certificate). The `wlst.sh` file is in the `bin` subdirectory of the `common` directory in the WebCenter Content Oracle home directory.

3.8.1 Configuring SSL for a Production Environment

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 Rights 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.

For information about configuring SSL for a production environment, see "SSL Configuration in Oracle Fusion Middleware" in the *Oracle Fusion Middleware Administrator's Guide*.

3.8.2 Configuring SSL for a Development Environment

For a development environment, you can also 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. After you configure one-way SSL for a development environment on the server, you have to configure every client to accept the server certificate.

3.8.2.1 Configuring One-Way SSL for a Development Environment

For a development environment, you might want to configure SSL, but it is not required. The application will work correctly without SSL configuration, but if you are using basic authentication or form-based authentication, credentials will be transferred from the client to the server unencrypted.

You can configure one-way SSL with a server certificate for the Managed Server so that the client application can be configured to trust the certificate.

In the following procedure, the `keystore` commands relate only to SSL and not to Oracle IRM encryption keys.

To configure one-way SSL for a development environment:

1. Run the `setWLSEnv` script to set the environment:

   - **UNIX script:**
     `MW_HOME/wlserver_10.3/server/bin/setWLSEnv.sh`

   - **Windows script:**
     `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` or `MW_HOME\wlserver_10.3\server\lib` directory.

2. Use the `CertGen` utility to create a server-specific, private key and certificate, as follows (in a single command line):

   ```
   java utils.CertGen -selfsigned
                   -certfile MyOwnSelfCA.cer
                   -keyfile MyOwnSelfKey.key
                   -keyfilepass mykeypass
                   -cn "hostname"
                   -keyusagecritical false
                   -keyusage digitalSignature,keyEncipherment,keyCertSign
   ```

   The last two lines are not needed for pure certificate use, but are needed if the certificate is also to be used for Java applications using Oracle Web Services over SSL.

For `mykeypass`, substitute a password for the key, and for *hostname,* substitute the name of the machine that hosts the Managed Server to which the application is deployed. You should use the same name while accessing Oracle Web Services. For example, to generate the server certificate for a machine named `myhost.us.example.com`, the command would be as follows (in a single command line):

```
java utils.CertGen -selfsigned
                  -certfile MyOwnSelfCA.cer
                  -keyfile MyOwnSelfKey.key
                  -keyfilepass mykeypass
                  -cn "myhost.us.example.com"
                  -keyusagecritical false
                  -keyusage digitalSignature,keyEncipherment,keyCertSign
```

This command will generate a server certificate for the machine `myhost.us.example.com`.

The parameter `-cn "` *machine-name*`"` must be set to the fully qualified domain name of the Managed Server to which the application is deployed. Oracle IRM will use this name to connect to the machine. Verify that the certificate has been issued to the machine name you specified.

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

3. Run the `ImportPrivateKey` utility to package the Private Key and Self-Signed Root Certificate into a key store, as follows (in a single command line):

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

Substitute an identity store password for `identitypass`, a key password for `keypassword`, and a key-file password for `mykeypass`.

4. Run the `keytool` utility to package the key and certificate into a separate key store named Trust Keystore.

In the following `keytool` commands (each a single command line), *JAVA_HOME* represents the location of the JDK. For information about the JAVA_HOME environment variable, see Section 2.3, "Installing an Application Server and Oracle Fusion Middleware."

- **UNIX operating system**

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

- **Windows operating system**

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

5. Click **Next**

On a Windows operating system, follow the instructions on the wizard screens.

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

a. Log in to the Oracle WebLogic Server Administration Console, 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.example.com: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 **Environment** 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**.

If the server is in production mode, you need to click the **Lock & Edit** button before you can make changes.

g. Enter values in the following fields on the **Keystores** tab:

Custom Identity Keystore

Custom Identity Keystore Type

Custom Identity Keystore Passphrase

Confirm Custom Identity Keystore Passphrase

Custom Trust Keystore

Custom Trust Keystore Type

Custom Trust Keystore Passphrase

Confirm Custom Trust Keystore Passphrase

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:

Private key alias

Private key passphrase

Confirm Private key passphrase

l. Save the changes.

If the server is running in development mode, then the changes need to be activated.

3.8.2.2 Configuring Clients to Accept the Server Certificate

After you create a server certificate to configure one-way SSL, you must install it on every machine running the client application. Then you can import the certificate into the client application so that it will trust the certificate and not show prompts when it connects to the Managed Server.

To configure clients to accept the server certificate:

1. 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.

    For a Windows operating system, the certificate file needs to be copied to the client machine that accesses this server through a browser.

    For a UNIX operating system that is accessing a web site over SSL rather than using the client application on the machine, follow the procedure required for your operating system to trust the certificate.

2. 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.

    On a Windows operating system, install the certificate under Trusted Root Certification Authorities in Internet Explorer.

3.9 Reassociating the Identity Store with an External LDAP Authentication Provider

In a production system, Oracle WebCenter Content 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, before you connect a Managed Server to a repository, and before the first user logs in to the application:

- Oracle Internet Directory
- Oracle Virtual Directory
- Third-party LDAP server

For an Imaging application, the user who logs in first to an Imaging Managed Server is provisioned with full security throughout the server. It is easier to reassociate the identity store for Imaging with an external LDAP authentication provider before the first user logs in, completes the configuration of the Imaging Managed Server, and connects it to the Oracle WebCenter Content repository.

For a Oracle IRM application, the Oracle IRM domain gets created the first time a user logs in to the Oracle IRM Management Console. A Oracle IRM domain is different from an Oracle WebLogic Server domain. The first user who logs in to the console is made the domain administrator for the Oracle IRM domain. Before you migrate user data for Oracle IRM, the users need to be in the target LDAP identity store. If you do not reassociate the identity store with an external LDAP authentication provider before the first user logs in to the Oracle IRM console, the general process for reassociating Oracle IRM users and migrating data follows:

1. Back up existing data with the `setIRMExportFolder` 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 `setIRMImportFolder` script.

3.9.1 Reassociating the Identity Store with Oracle Internet Directory

You can reassociate the identity store for an Oracle WebLogic Server domain with Oracle Internet Directory and migrate 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 3–5 lists the available authenticator types.

Table 3–5   LDAP Authenticator Types

LDAP Authentication Provider	Authenticator Type
Microsoft AD	ActiveDirectoryAuthenticator
SunOne LDAP	IPlanetAuthenticator
Directory Server Enterprise Edition (DSEE)	IPlanetAuthenticator
Oracle Internet Directory	OracleInternetDirectoryAuthenticator
Oracle Virtual Directory	OracleVirtualDirectoryAuthenticator
EDIRECTORY	NovellAuthenticator
OpenLDAP	OpenLDAPAuthenticator
EmbeddedLDAP	DefaultAuthenticator

To reassociate the identity store with Oracle Internet Directory:

1. Ensure that there is no user in Oracle Internet Directory with the same name as the administrator of the Oracle WebLogic Server domain, which is `weblogic` by default.

2. Set both embedded and external LDAP providers to `SUFFICIENT`.

3. For Oracle IRM, log in to the management console as a user from Oracle Internet Directory, to be the Oracle IRM domain administrator.

   Do not log in to the management console with the user name of the Oracle WebLogic Server domain administrator. The Oracle recommendation is to not use the `weblogic` user account as the Oracle IRM administration user account. If you use a different account for the Oracle IRM domain administrator, you can use the Oracle WebLogic Server domain administrator, `weblogic` by default, to start and stop Oracle WebLogic Server as well as to alter server settings. If you have a problem with Oracle Internet Directory, you will not need to fix it before you can do maintenance on Oracle WebLogic Server.

4. For a Oracle IRM Managed Server, if a user has already logged into the Oracle IRM Management Console, you need to run the WebLogic Scripting Tool (WLST) `setIRMExportFolder` command before identity store reassociation.

   Use this command to set an export folder for exporting the user and group details referenced by Oracle IRM, which uses the export folder path to decide where to write out the user and group details. The Oracle IRM Managed Server must have write access to the folder path. The export folder must exist before you run the `setIRMExportFolder` command.

The following example sets `/scratch/irm-data` as the export folder:

```
cd WC_CONTENT_ORACLE_HOME/common/bin
./wlst.sh
> connect('weblogic', 'password', 't3://adminServerHost:adminServerPort')
> setIRMExportFolder('/scratch/irm-data')
```

In the example, *adminServerHost* is the host name and *adminServerPort* is the port number for the Administration Server of the Oracle WebLogic Server domain.

> **Note:** If SSL is enabled, before you use WLST to connect to the Administration Server, you must either append the following parameters to the JVM_ARGS section of the `wlst.sh` file or set them in the CONFIG_JVM_ARGS environment variable:
>
> ```
> -Dweblogic.security.SSL.ignoreHostnameVerification=true
> -Dweblogic.security.TrustKeyStore=KeyStoreName
> ```
>
> *KeyStoreName* is the name of the keystore in use (`DemoTrust` for the built-in demonstration certificate). The `wlst.sh` file is in the `bin` subdirectory of the `common` directory in the WebCenter Content Oracle home directory.

After the Oracle IRM Managed Server picks up this configuration change, normally right away, it will write out a series of XML documents in the export folder. This process is complete when a folder named `accounts` appears under the export folder. The `accounts` folder will contain one or more folders named `batch`*XXX*, with each batch folder containing a set of XML documents that include the user and group details. For example:

```
/scratch
    /irm-data
        /accounts
            /batch1
                user1.xml
                user2.xml
                group1.xml
```

The batch folders are used to ensure that the operating system limit of the maximum number of files in a folder is not exceeded.

After this process is complete, reset the export folder:

```
setIRMExportFolder('')
```

This reset ensures that Oracle IRM does not perform any further data exporting when the Managed Server restarts.

5. Configure the Oracle Internet Directory authentication provider:

    a. Start the Administration Server for your Oracle WebLogic Server domain, as described in Section 9.1, "Starting the Administration Server."

    b. Log in to the Oracle WebLogic Server 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.example.com: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 3–5.

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.

The **Configuration** tab has two tabs, **Common** and **Provider Specific**. On the **Common** tab, 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 the 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 the 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.

  For Oracle IRM, select this attribute in the General area of the tab.

  l. Click **Save**.

6. 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.

---

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

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

9. 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.

10. 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 9.2, "Starting Managed Servers."

11. 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.

12. Restart the Administration Server and the Managed Server, as described in Section 9.3, "Restarting a Managed Server."

13. For a Oracle IRM Managed Server, if a user has already logged into the Oracle IRM Management Console, you need to run the setIRMImportFolder WLST command after identity store reassociation. Use this command to set the import folder to point to the export folder that was set before identity store reassociation.

> **Note:** You should take a backup of the export folder before performing the import process because the import process deletes the contents of the folder during successful processing of the user and group details.

This operation should be performed with only one Managed Server running a deployed Oracle IRM application, to ensure that only one Managed Server performs the user and group processing. After the import process is complete, all Managed Servers running the Oracle IRM application can be started.

The following example sets /scratch/irm-data as the import folder:

```
cd WC_CONTENT_ORACLE_HOME/common/bin
./wlst.sh
> connect('weblogic', 'password', 't3://adminServerHost:adminServerPort')
> setIRMImportFolder('/scratch/irm-data')
```

After the Oracle IRM Managed Server picks up this configuration change, it will read the contents of the folder and update the global user ID (GUID) values in the Oracle IRM system to reflect the values in the new identity store. When a user or group has been processed, the import process deletes the corresponding XML file. After the import process is complete, the import folder will be empty:

```
/scratch
    /irm-data
```

If an error occurs during the processing of a user or group, the import process writes the error to a file that matches the user or group name. For example, if the user details in `user1.xml` cause an error during processing, the import process writes the error details to the file `user1.xml.fail`:

```
/scratch
    /irm-data
        /accounts
            /batch1
                user1.xml
                user1.xml.fail
```

If you can fix the error, then rerun the `setIRMImportFolder` WLST command to rerun the import process. For example, if user or group processing fails because the user or group does not exist in the new identity store, adding the user or group to Oracle Internet Directory will fix the error, and you can rerun the import process:

```
> connect('weblogic', 'password', 'adminServerHost:adminServerPort')
> setIRMImportFolder('/scratch/irm-data')
```

After this process is complete, reset the import folder:

```
setIRMImportFolder('')
```

This reset ensures that Oracle IRM does not perform any further data importing when the Managed Server restarts.

> **Note:** When reassociating an LDAP identity store, the Oracle IRM process for exporting user and group information has an issue if user and group names are identical. If a user and group have identical names, the export process will lose either the user or the group details during the export step. This is because the user or group name is used as the file name, so one file overwrites the other. A postreassociation workaround is to check user and group right assignments, and to manually reassign any that are missing.

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 a 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.

3.9.2 Refreshing GUID Values in Imaging Security Tables

If you change the LDAP providers, the global user IDs (GUIDs) in the Imaging security tables will be invalid. Imaging caches the GUIDs from an external LDAP provider in its local security tables and uses these IDs for authentication. You can refresh the GUID values in the Imaging security tables with WLST commands or with Fusion Middleware Control.

Only users and groups that exist in both LDAP providers will have GUIDs refreshed. Imaging permissions assigned to users and groups from the previous LDAP will be refreshed to the users and groups that match in the new LDAP. If users and/or groups

do not match any users and/or groups in the new LDAP provider, refreshIPMSecurity will ignore them.

> **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 Imaging database.

3.9.2.1 Refreshing GUID values in Imaging Security Tables with WLST

If you want to refresh GUID values from a command line, you can use Oracle WebLogic Scripting Tool (WLST).

To refresh GUID values in Imaging security tables with WLST:

1. Log in to Oracle WebLogic Server Administration Server.

2. Navigate to the Oracle WebCenter Content home directory: *MW_HOME/WC_CONTENT_ORACLE_HOME*.

3. Invoke WLST:

```
cd common/bin
./wlst.sh
```

4. At the WLST command prompt, enter these commands:

```
wls:/offline> connect()
Please enter your username :weblogic
Please enter your password : XXXXXXXXXXXXX
Please enter your server URL [t3://localhost:7001]
 :t3://host_name:16000
Connecting to t3://host_name:16000 with userid weblogic ...
Successfully connected to Managed Server 'IPM_server1' that belongs to domain
'domainName'.

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:/domainName/serverConfig> listIPMConfig()   <This is just to check
that the connection is to the right Imaging server>

wls:/domainName/serverConfig>
refreshIPMSecurity()  <This is the command that will refresh the GUIDs in the
Security tables.>

wls:/domainName/serverConfig> exit()
```

5. Log in to Imaging to verify user and group security.

3.9.2.2 Refreshing GUID values in Imaging Security Tables with Fusion Middleware Control

If you want to refresh GUID values through an MBean, you can use the System MBean Browser in Fusion Middleware Control.

To refresh GUID values in Imaging security tables with Fusion Middleware Control:

1. Log in to Fusion Middleware Control.

2. In the navigation tree on the left, expand **WebLogic Domain**, then the Oracle WebCenter Content domain folder, then **IPM_Cluster**, and then the name of the Imaging server, such as **IPM_server1**.

3. On the right, click the **WebLogic Server** drop-down menu, and choose **System MBean Browser**.

4. In the System MBean Browser navigation tree, expand **Application Defined MBeans**, then **oracle.imaging**, then **Server: IPM_server1**, and then **cmd**, and click **cmd**.

5. Click **refreshIPMSecurity** on the right.

6. Press the **Invoke** button.

7. Log in to Imaging to verify user and group security.

3.10 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 the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*. For more information about entries, see "Managing Directory Entries" in the *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 the *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.

3.11 Installing Fonts for National Language Support on a UNIX System

For languages other than English, the following installation steps need to be done on a UNIX operating system before you start a Managed Server:

- Copy *MW_HOME*`/oracle_common/jdk/jre/lib/fonts` to the `/jre/lib/fonts` directory in the Sun JDK installation directory for the Middleware home.

- Copy *MW_HOME*`/oracle_common/jdk/jre/lib/fonts` to the `/jre/lib/fonts` directory in the Oracle JRockit JDK directory for the Middleware home.

3.12 Configuring Single Sign-On (SSO)

You can configure one of these single sign-on (SSO) solutions for an Oracle WebCenter Content product:

- Oracle Access Manager 11g SSO
- Oracle Access Manager 10g SSO
- Oracle Single Sign-On (OSSO)
- Windows Native Authentication (WNA)

Table 3–6 shows which SSO solutions you can use with which Oracle WebCenter Content applications. The sections that follow provide references to information about using SSO with these applications.

Table 3–6   Single Sign-On Solutions for Oracle WebCenter Content Applications

Application	Oracle Access Manager 11g	Oracle Access Manager 10g	OSSO	WNA
WebCenter Content, with Content Server	Supported	Supported	Supported	Supported
Imaging	Supported	Supported	Supported	Supported
Oracle IRM Web Interface	Supported	Not supported	Supported	Supported
Rights Desktop	Not supported	Supported (limited)	Not supported	Supported
Records	Supported	Supported	Supported	Supported

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

3.12.1 Configuring Oracle Access Manager Single Sign-On

Oracle Access Manager enables users to seamlessly gain access to web applications and other IT resources across your enterprise. Oracle IRM supports Basic authentication with Oracle Access Manager, which contains an authorization engine that 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.

For information about configuring Oracle Access Manager single sign-on (SSO) for Oracle IRM, see Section 7.4, "Integrating Rights with Oracle Access Manager 11g." For information about configuring it for Imaging, see the *Oracle WebCenter Content Administrator's Guide for Imaging*. For information about configuring it for WebCenter Content, Inbound Refinery, or Records, see "Configuring Oracle WebCenter Content for Single Sign-On" in the *Oracle WebCenter Content System Administrator's Guide for Content Server*.

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

Table 3–7 shows where to get more information about configuring Oracle Access Manager 11*g* for Oracle WebCenter Content applications.

Table 3–7   Oracle Access Manager 11g Configuration for Oracle WebCenter Content Applications

Application	Configuration Information
WebCenter Content, with Content Server	"Configuring Oracle Access Manager 11g with Oracle WebCenter Content" in *Oracle WebCenter Content System Administrator's Guide for Content Server*
Imaging	"Integrating Oracle Access Manager 11g with Imaging" in *Oracle WebCenter Content Administrator's Guide for Imaging*
Oracle IRM Web Interface	Section 7.4, "Integrating Rights with Oracle Access Manager 11g"
Rights Desktop	Not supported
Records	"Configuring Oracle Access Manager 11g with Oracle WebCenter Content" in *Oracle WebCenter Content System Administrator's Guide for Content Server*

Table 3–8 shows where to get more information about configuring Oracle Access Manager 10*g* for Oracle WebCenter Content applications.

Table 3–8   Oracle Access Manager 10g Configuration for Oracle WebCenter Content Applications

Application	Configuration Information
WebCenter Content, with Content Server	"Configuring Oracle Access Manager 10g with Oracle WebCenter Content" in *Oracle WebCenter Content System Administrator's Guide for Content Server*
Imaging	"Integrating Oracle Access Manager 10g with Imaging" in *Oracle WebCenter Content Administrator's Guide for Imaging*
Oracle IRM Web Interface	Not supported
Rights Desktop	Section 7.4, "Integrating Rights with Oracle Access Manager 11g"
Records	"Configuring Oracle Access Manager 11g with Oracle WebCenter Content" in *Oracle WebCenter Content System Administrator's Guide for Content Server*

3.12.2 Configuring Oracle Single Sign-On

For an overview of Oracle Single Sign-On (OSSO), see "Introduction to Single Sign-On in Oracle Fusion Middleware" in the *Oracle Fusion Middleware Application Security Guide*.

Table 3–9 shows where to get more information about configuring OSSO for Oracle WebCenter Content applications.

Table 3–9   OSSO Configuration for Oracle WebCenter Content Applications

Application	Configuration Information
WebCenter Content, with Content Server	"Configuring Oracle Single Sign-On for Oracle WebCenter Content" in *Oracle WebCenter Content System Administrator's Guide for Content Server*
Imaging	"Configuring Oracle Single Sign-On for Imaging" in *Oracle WebCenter Content Administrator's Guide for Imaging*
Oracle IRM Web Interface	"Configuring Single Sign-On using OracleAS SSO 10g" in *Oracle Fusion Middleware Application Security Guide*
Rights Desktop	Not supported
Records	"Configuring Single Sign-On using OracleAS SSO 10g" in *Oracle Fusion Middleware Application Security Guide*

3.12.3 Configuring Windows Native Authentication

For information about configuring Windows Native Authentication (WNA), see "Configuring Single Sign-On with Microsoft Clients" in the *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

Table 3–10 shows where to get more information about configuring WNA for Oracle WebCenter Content applications.

Table 3–10   WNA Configuration for Oracle WebCenter Content Applications

Application	Configuration Information
WebCenter Content, with Content Server	"Configuring Oracle WebCenter Content and Single Sign-On for Windows Native Authentication" in *Oracle WebCenter Content System Administrator's Guide for Content Server*
Imaging	"Configuring Imaging and Single Sign-On for Windows Native Authentication" in *Oracle WebCenter Content Administrator's Guide for Imaging*
Oracle IRM Web Interface	"Configuring Single Sign-On with Microsoft Clients" in *Oracle Fusion Middleware Securing Oracle WebLogic Server*
Rights Desktop	"Configuring Single Sign-On with Microsoft Clients" in *Oracle Fusion Middleware Securing Oracle WebLogic Server*
Records	"Configuring Single Sign-On with Microsoft Clients" in *Oracle Fusion Middleware Securing Oracle WebLogic Server*

3.13 Integrating Oracle Web Tier with WebCenter Content

Oracle recommends using Oracle Web Tier (Oracle HTTP Server) for Content Server integration with Site Studio, single sign-on (SSO), and clusters. You can install and configure Oracle Web Tier (OHS) 11*g* as an alternative to the Oracle Weblogic Server HTTP listener.

For information about installing and Oracle Web Tier (OHS), see "Installing and Configuring the Oracle HTTP Server" in the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal*.

3.14 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 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.

> **Note:**   To use clusters, you need a license for Oracle WebLogic Server Enterprise Edition.

For an overview of clusters, see "Understanding WebLogic Server Clustering" in the *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 that Table 3–11 describes.

Table 3–11   Managed Servers, Clusters, and Machines Advanced Settings Screens

Screen	Description and Action Required
Configure Managed Servers	Add new Managed Servers, or edit and delete existing Managed Servers.
	Click **Next** to continue.
Configure Clusters	Create clusters if you are installing in a high availability environment. For more information, see the *Oracle Fusion Middleware High Availability Guide*.
	Click **Next** to continue.
Assign Servers to Clusters	If you configured any clusters on the Configure Clusters screen
	Click **Next** to continue.
Create HTTP Proxy Applications	If you configured any clusters on the Configure Clusters screen and assigned some, but not all, of the Managed Servers in the domain to a cluster
	Click **Next** to continue.
Configure Machines	Configure the machines that will host the Managed Servers in a cluster, and assign each Managed Server to a machine.
	Click **Next** to continue.
Target Deployments to Clusters or Servers	Assign your Managed Servers to clusters or servers in your domain.
	Click **Next** to continue.
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 Oracle WebLogic Server Administration Console or Fusion Middleware Control. For more information, see "Scaling Your Environment" in the *Oracle Fusion Middleware Administrator's Guide*.

3.15 Setting Up Oracle Web Services Manager Security

To set up Oracle Web Services Manager (Oracle WSM) security policies for Oracle WebCenter Content, you need to do these tasks:

1. Installing Oracle WebLogic Server and Oracle WebCenter Content

2. Creating an Oracle WSM MDS Schema with the Repository Creation Utility

3. Configuring Oracle WebCenter Content Applications and Oracle WSM Policy Manager in an Oracle WebLogic Server Domain

4. Configuring the Server Socket Port and Incoming Socket Connection Address Security Filter for Oracle WSM

5. Securing Web Services with a Key Store and Oracle WSM Policies

3.15.1 Installing Oracle WebLogic Server and Oracle WebCenter Content

Install Oracle WebLogic Server with the **Typical** option, which also installs Oracle Coherence and the Sun and JRockit JDKs. For information about how to install Oracle WebLogic Server, see Section 2.3, "Installing an Application Server and Oracle Fusion Middleware."

The installation of Oracle WebLogic Server creates an Oracle Fusion Middleware home, where you can install Oracle WebCenter Content, which creates a WebCenter Content Oracle home. Oracle WSM can be installed from Oracle WebCenter Content. The Middleware home includes an Oracle Common home, where the Oracle WSM files are installed. For information about how to install Oracle WebCenter Content, with the files necessary for deploying Oracle WebCenter Content, applications, see Section 2.4, "Using the Installer for Oracle WebCenter Content."

3.15.2 Creating an Oracle WSM MDS Schema with the Repository Creation Utility

Make the following selection on the RCU Select Components screen to create the MDS schema, which you need for setting up Oracle WSM security:

Metadata Services under **AS Common Schemas**

The selection is for creating an Oracle WSM Policy Manager schema. This schema will provide a back-end repository for WebCenter Content, with Content Server and the Oracle WSM Policy Manager. If an MDS schema already exists in your database, you can reuse the schema.

For more information about creating the Oracle WSM MDS schemas with RCU, see Section 2.2, "Creating Oracle WebCenter Content Schemas with the Repository Creation Utility."

3.15.3 Configuring Oracle WebCenter Content Applications and Oracle WSM Policy Manager in an Oracle WebLogic Server Domain

To configure one or more Oracle WebCenter Content applications and Oracle WSM Policy Manager, you need to create or extend an Oracle WebLogic Server domain. For information about creating a domain to include Oracle WSM Policy Manager, see Section 3.2, "Creating an Oracle WebLogic Server Domain." For information about extending a domain with Oracle WSM Policy Manager, see Section 3.3, "Extending an Existing Domain."

3.15.4 Configuring the Server Socket Port and Incoming Socket Connection Address Security Filter for Oracle WSM

During post-installation configuration of a Managed Server, you can configure the **Server Socket Port** and **Incoming Socket Connection Address Security Filter** values for Oracle WSM.

Make sure that the following settings exist along with other default settings:

- **Server socket port:** `4444`

  This value is stored in the configuration file for the Managed Server as `IntradocServerPort=4444`.

- **Incoming Socket Connection Address Security Filter:**
  `*.*.*|0:0:0:0:0:0:0:1`

  This value is stored in the configuration file for the Managed Server as `SocketHostAddressSecurityFilter=*.*.*|0:0:0:0:0:0:0:1`.

Before any changes to these settings take effect, you need to restart the Managed Server, as described in Section 9.3, "Restarting a Managed Server."

For more information about the post-installation configuration of a Managed Server, see one or more of these sections:

- Section 4.3, "Completing the Initial Configuration of Content Server"

- Section 5.1, "Completing the Initial Inbound Refinery Configuration"

- Section 6.1, "Completing the Initial Imaging Configuration"

- Section 7.1, "Completing the Initial Oracle IRM Configuration"

- Section 8.1, "Completing the Initial Records Configuration"

3.15.5 Securing Web Services with a Key Store and Oracle WSM Policies

To secure web services, you can set up a key store and apply Oracle WSM policies to the web services.

3.15.5.1 Setting Up a Key Store

The `keytool` command will generate a key store, which requires a password to open. Inside the key store, a key will be stored, and access to the key requires an additional password.

The suggested location for the key store is in a directory under the domain home:

- **UNIX path:**
  `MW_HOME/user_projects/domains/DomainHome/config/fmwconfig`

- **Windows path:**
  `MW_HOME\user_projects\domains\DomainHome\config\fmwconfig`

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 set up a key store:

1. Creating the key store and key alias `orakey`:

   ```
   JAVA_HOME/bin/keytool -genkeypair -alias orakey -keypass welcome -keyalg RSA \
                         -dname "CN=orakey, O=oracle C=us" \
                         -keystore default-keystore.jks -storepass welcome
   ```

2. Copy `default-keystore.jks` to the domain's `fmwconfig` directory:

   ```
   cp default-keystore.jks DomainHome/config/fmwconfig
   ```

3. Save the credentials in a credential store (using WLST commands):

   ```
   MW_HOME/WC_CONTENT_ORACLE_HOME/common/bin/wlst.sh
   connect()
   createCred(map="oracle.wsm.security", key="keystore-csf-key", user="keystore",
   password="welcome1")
   createCred(map="oracle.wsm.security", key="sign-csf-key", user="orakey",
   password="welcome")
   createCred(map="oracle.wsm.security", key="enc-csf-key", user="orakey",
   password="welcome1")
   ```

   This step creates a file, `cwallet.sso`, under `DomainHome/config/fmwconfig`.

Both `default-keystore.jks` and `cwallet.sso` are needed for the client to access the server.

For more information about setting up a key store, see Section 7.1.2, "Configuring a Key Store for Oracle IRM."

3.15.5.2 Applying Oracle WSM Policies to Web Services

The following procedure shows how to apply a policy to the WebCenter Content Web Services, with `IdcWebLoginService` and `GenericSoapService`. The policy to be applied is `oracle/wss11_saml_token_with_message_protection_service_policy`

You can use the Oracle WebLogic Server Administration Console to handle the application of Oracle WSM policies to web services

To apply an Oracle WSM policy to a web service:

1. Log in to the Oracle WebLogic Server Administration Console as the Oracle WebLogic Server administrator.

2. Click **Deployments** in the navigation tree on the left.

3. In the Deployments table, page to **Oracle WebCenter Content Native Web Services**, and expand it.

4. Click **IdcWebLoginService**.

5. On the Settings for IdcWebLoginService page, click **Configuration**.

6. Select the **WS-Policy** tab.

7. Apply the OWSM policy `oracle/wss11_saml_token_with_message_protection_service_policy` to `IdcWebLoginPort`.

4

Completing the WebCenter Content Configuration

This chapter explains how to complete the initial configuration of Oracle WebCenter Content, with Oracle WebCenter Content Server, in an Oracle WebLogic Server domain.

This chapter includes the following sections:

- Section 4.1, "Configuring the Report Library for Records Management in Content Server"
- Section 4.2, "Completing the Initial WebCenter Content Configuration"
- Section 4.3, "Completing the Initial Configuration of Content Server"
- Section 4.4, "Configuring OracleTextSearch for Content Server"
- Section 4.5, "Configuring a JDBC Driver for Standalone Applications"
- Section 4.6, "Importing a Database Root CA Certificate into the Key Store for a Standalone Application"
- Section 4.7, "Enabling and Configuring Site Studio on Content Server"
- Section 4.8, "Configuring Content Server for Desktop"
- Section 4.9, "Installing and Configuring Desktop on a Client Workstation"
- Section 4.10, "Opening Files from Microsoft Office 2010 Over a Non-SSL Connection"
- Section 4.11, "Configuring Records Management in Content Server"
- Section 4.12, "Configuring Oracle Application Extension Framework"
- Section 4.13, "Installing and Configuring Oracle Document Capture and Oracle Distributed Document Capture"

4.1 Configuring the Report Library for Records Management in Content Server

If you plan to configure the Records Management feature in Content Server, you need configure the report library for Records Management after creating the domain that includes the WebCenter Content Managed Server, before starting it for the first time. Without this library, you cannot check in any templates to Content Server.

To configure the report library, you need to add the `oracle.xdo.runtime` library manually from the Oracle WebLogic Server Administration Console and then add a reference to this library in the `weblogic-application.xml` file of the WebCenter Content EAR.

> **Note:** This library is not needed for Oracle WebCenter Content: Records.

To add the oracle.xdo.runtime.ear library to the WebCenter Content Managed Server:

1. After a domain is created, start only the Administration Server.

   If the WebCenter Content Managed Server has already been started, then you will have to perform additional steps to add a reference to the deployed WebCenter Content instance later.

2. Open the Administration Console in browser, click **Deployments** on the left, and browse the pages to check if there is already an `oracle.xdo.runtime` file. If it is already present, then no more steps need to be performed.

3. If the `oracle.xdo.runtime` file does not already exist, click **Install** on the Deployments display. A file selection dialog opens. Browse the available file system, and select the following path:

   MW_HOME/WC_CONTENT_ORACLE_HOME/ucm/idc/components/ReportPublisher/lib/

4. Click **Next**. The option page to select the file as library opens. Select **Install this deployment as a library**, and click **Next**.

5. The Target Selection Screen opens. Select all targets, and click **Next**.

6. The Deployment Name screen opens. In the Security section, select **DD Only: Use only roles and policies that are defined in the deployment descriptors.** In the Source accessibility section, select **Copy this application onto every target for me**, and click **Next**.

7. In the Additional Configuration section, select **Yes, Take me to the deployment's configuration screen**, and click **Finish**. The library is now deployed in the environment.

To reference the deployed library from the UCM Enterprise Application library:

1. Extract the `cs.ear` file from the following path:

   MW_HOME/WC_CONTENT_ORACLE_HOME/ucm/idc/components/ServletPlugin/cs.ear

2. In the extracted directory, modify `META-INF/weblogic-application.xml`, and add the following library reference:

   ```
   <library-ref>
       <library-name>oracle.xdo.runtime</library-name>
   </library-ref>
   ```

3. Create an archive file named `cs.ear` from the extracted, modified directory, and replace the file of the same name in the path it was retrieved from. This change will take effect for all undeployed WebCenter Content instances.

4. If this is not the first time the WebCenter Content Managed Server has been started since the domain was created, you need to perform these additional steps:

   a. Locate the `weblogic-application.xml` file of the WebCenter Content application in the deployed WebCenter Content Managed Server, with a path like this:

      ```
      DomainHome/servers/WC_CONTENT_servername/tmp/_WL_user/Oracle WebCenter
      Content - Content Server/k6ggd/META-INF/weblogic-application.xml
      ```

      If the name of the WebCenter Content Managed Server is not in the `DomainHome/servers` directory, then these additional steps are not necessary because the Managed Server has not been started, which would have deployed it at this location.

   b. Modify the `META-INF/weblogic-application.xml` file, and add the following line for library reference:

      ```
      <library-ref>
          <library-name>oracle.xdo.runtime</library-name>
      </library-ref>
      ```

   c. Start the WebCenter Content Managed Server, as described in Section 9.3, "Restarting a Managed Server."

5. Start the WebCenter Content Managed Server, as described in Section 9.2, "Starting Managed Servers."

   If the Managed Server has been started before, restart it, as described in Section 9.3, "Restarting a Managed Server."

For information about adding the Records Management feature to Content Server, see Section 4.11, "Configuring Records Management in Content Server"

4.2 Completing the Initial WebCenter Content Configuration

After you start the Administration Server and Oracle WebCenter Content Managed Server, as described in Chapter 9, "Verifying the Oracle WebCenter Content Configuration," you can complete the WebCenter Content configuration on the postinstallation configuration page in Content Server.

The first user to log in to Oracle WebCenter Content Server must be the administrator of the Oracle WebLogic Server domain, to complete the configuration of Content Server. For more information, see Section 9.6, "Verifying the Configuration of Oracle WebCenter Content," and also see "Introduction to Content Server Administration," "Managing Security and User Access," and "Starting, Stopping, and Restarting Content Server" in the *Oracle WebCenter Content System Administrator's Guide for Content Server*.

WebCenter Content displays the Content Server Configuration page when you first log in to Content Server at

```
http://managedServerHost:managedServerPort/cs
```

When you configure WebCenter Content on the same machine and in the same Oracle WebLogic Server domain as Imaging, the postinstallation configuration of WebCenter Content is done automatically. If you follow the default configuration for the

installation of WebCenter Content and Imaging, both applications are installed on the same machine. In this environment, Imaging provides a configuration file that sets up WebCenter Content for use by Imaging.

If WebCenter Content is intended to be used as a full Managed Server in addition to servicing Imaging, then the WebCenter Content administrator should review the automatic configurations through the administration interfaces in Content Server. The additional configuration steps described in the rest of this chapter should be done on the WebCenter Content Managed Server to fully configure it for production.

The Imaging administrator should verify that the default WebCenter Content configurations are correct for use by the Imaging Managed Server. For Imaging use, many of the WebCenter Content postinstallation configuration steps, such as configuring Oracle WebCenter Content: Inbound Refinery, are not required.

Before you can use Inbound Refinery with WebCenter Content, you need to configure Inbound Refinery for document and image conversions to work with Content Server. For transformations to work on some platforms, certain environment variables must be set before you start the Managed Server. For more information, see Section 3.7.2, "Setting Library Paths in Environment Variables on UNIX Platforms."

To complete the WebCenter Content configuration:

1. Start the Administration Server, as described in Section 9.1, "Starting the Administration Server."

2. Start the WebCenter Content Managed Server, as described in Section 9.2, "Starting Managed Servers."

3. Browse to the Content Server postinstallation configuration page, at this web site:

   ```
   http://managedServerHost:16200/cs/
   ```

   > **Important:** The first user to log in to Oracle WebCenter Content Server must be the administrator of the Oracle WebLogic Server domain, to complete the configuration of Content Server. For more information, see Section 9.6, "Verifying the Configuration of Oracle WebCenter Content," and also see "Introduction to Content Server Administration," "Managing Security and User Access," and "Starting, Stopping, and Restarting Content Server" in the *Oracle WebCenter Content System Administrator's Guide for Content Server*.

4. Enter or edit any configuration values you want to change.

   In the **FullText Search Option** field, you can select a full-text search engine. Leaving it blank will set up the system as metadata only.

   For information about the values to enter, see Section 4.3, "Completing the Initial Configuration of Content Server."

5. To enable access from Inbound Refinery, provide a value for **Incoming Socket Connection Address Security Filter**, as follows:

   ```
   127.0.0.1|your.server.IP.address|::1
   ```

   This field accepts wildcards in the value, like 10.*.*.*. You can change this value later by setting SocketHostAddressSecurityFilter in DomainHome/ucm/cs/config/config.cfg and restarting Content Server.

For Oracle WSM security, the `SocketHostAddressSecurityFilter` value needs to set to like this:

```
SocketHostAddressSecurityFilter=*.*.*.*|0:0:0:0:0:0:0:1
```

For more information, see Section 3.15.4, "Configuring the Server Socket Port and Incoming Socket Connection Address Security Filter for Oracle WSM."

6. If you want to set up a provider from Inbound Refinery back to Content Server, enter an unused port number, such as `4444`, for **Server Socket Port**.

   You can change this value later by setting `IntradocServerPort` in *DomainHome*`/ucm/cs/config/config.cfg` and restarting Content Server.

7. Click **Submit**.

8. Restart Content Server, as described in Section 9.3, "Restarting a Managed Server."

4.3 Completing the Initial Configuration of Content Server

After installing and configuring WebCenter Content on an Oracle WebLogic Server Managed Server, you need to complete the initial configuration of Content Server. Completing its initial configuration includes these tasks:

- Starting Content Server
- Configuring the Content Server Instance
- Enabling or Disabling Components
- Configuring the Folders Interface
- Configuring Content Server for IBM DB2 Database Searches
- Configuring Microsoft SQL Server to Work with WebCenter Content

For information about changing the configuration of Content Server and additional configuration options, see "Configuring Content Server" in the *Oracle WebCenter Content System Administrator's Guide for Content Server*.

4.3.1 Starting Content Server

You can start WebCenter Content, which includes Content Server, with the Oracle WebLogic Server Administration Console, the `startManagedWebLogic` startup script, or Oracle Enterprise Manager Fusion Middleware Control.

For more information, see "Starting Content Server" in the *Oracle WebCenter Content System Administrator's Guide for Content Server*.

4.3.2 Configuring the Content Server Instance

Figure 4–1 shows the configuration page for Content Server.

Figure 4–1   Configuration Page for Content Server

The following table describes the fields on this page and the values you can enter to configure your Content Server instance.

Field	Description
Cluster Node Identifier	The name of the WebCenter Content Managed Server where Content Server will run.

Field	Description
Content Server Instance Folder	The absolute path to the Oracle instance directory for Content Server. Oracle recommends that you specify an instance directory that is outside of the Domain home.
	The default Oracle instance directory for Content Server follows:
	`MW_HOME/user_projects/domains/`*DomainHome*`/ucm/cs`
	The name of the top-level folder in the folder hierarchy for the Content Server instance is `cs`.
	The path to the Oracle instance directory is the value of the `IntradocDir` variable for the Content Server instance. This directory path should be unique to this particular Managed Server, or node. For installations that are likely to be upgraded to future versions of the product, Oracle strongly recommends that you change the location of the Oracle instance directory to a directory outside of any Oracle WebLogic Server domain directories or installation directories. For installations that will be in a cluster, the Oracle instance directory must be on a network to which all nodes in the cluster have shared access.
Native File Repository Location	The path to the vault directory for storing native content checked into Content Server.
Weblayout Folder	The path to the weblayout directory for storing web-viewable renditions of native and alternate files.
Content Server URL Prefix	The relative URL for the Content Server instance.
Is New Content Server Instance	Whether or not the Content Server instance is a new one.
Server Socket Port	The number of the port for calling top-level services. The default value is blank.
	Changing this field value changes the `IntradocServerPort` entry in *DomainHome*`/ucm/cs/config/config.cfg`. The default `IntradocServerPort` value is blank.
Incoming Socket Connection Address Security Filter	Restricts Content Server access to a computer or computers with a specified IP address or addresses.
	■ By default, this field is prefilled with the IP address of the local host (`127.0.0.1`).
	■ You can specify multiple IP addresses, separated by pipes (`|`). Make sure that there are no spaces on either side of the pipe character. (For example: `127.0.0.1|0:0:0:0:0:0:0:1|192.168.1.1`)
	■ You can use wildcards in this field, * for zero or many characters, and ? for any one character. (For example, `10.10.3.*`)
	■ Generally, use only the **IP Address Filter** field or **Hostname Filter** field, not both. (**IP Address Filter** is more commonly used.)
Web Server HTTP/HTTPS Address	The name of the web server. (`HttpServerAddress` property).
Web Address Is HTTPS	Whether or not the URL for the web server starts with `HTTPS`, for a Managed Server that has SSL enabled.

Field	Description
Company Mail Server	An email server that Content Server can use to send email notifications.
	This value generally takes the form of *mail.example.com*. If applicable, make sure to allow for sending email through a firewall.
Administrator E-Mail Address	An email address that Content Server can use to send email notifications (`SysAdminAddress`).
	This address will receive a returned message for any delivery failure that occurs.
Server Instance Name	The name of the Content Server instance.
	This name should contain only letters, numerals, and underscore characters. Other characters can cause problems. For example, an instance name that contains periods can cause a JavaScript error if the name is used to create a JavaScript variable.
Server Instance Label	The instance name that is displayed in the Windows **Start** menu (`InstanceMenuLabel` property).
Server Instance Description	A description of the Content Server instance (`InstanceDescription` property).
Is Auto Number Enabled	Whether or not automatic numbering of Content Server instances is enabled.
Auto Number Prefix	A unique prefix for a Content Server instance number, to avoid conflicts among multiple Content Server instances (Auto Number Prefix system property).
FullText Search Option	Specifies the search engine for full-text searches:
	■ **None**: The Content Server instance will use `DATABASE.METADATA` as the search engine.
	■ **Internal**: For Oracle Database 11*g*, the Content Server instance will use `OracleTextSearch` with the system database. For Microsoft SQL Server, Content Server will use `DATABASE.FULLTEXT`. For IBM DB2, Content Server will use `DATABASE.METADATA`.
	■ **External**: The Content Server instance will use `OracleTextSearch` with an external data source in an Oracle Database (not the system database), SQL Server, or IBM DB2. If you select this option, you must provide the name of the external data source in the **External DataSource** field.

Field	Description
External DataSource	The name of an external data source that was created and targeted through the Administration Console to the WebCenter Content Managed Server, using an OCSSEARCH schema that was created with Repository Creation Utility (RCU).
	For information about creating an external data source and targeting it to a Managed Server, see "How to Create a JDBC Data Source for Oracle WebLogic Server" in the *Oracle Fusion Middleware Java EE Developer's Guide for Oracle Application Development Framework*.
	You can specify the name of an external provider for the data source. For information about creating an external provider, see Section 4.4.2, "Configuring an External Database Provider for Standalone Applications."
	If the external data source is for use with IBM DB2, also see Section 4.3.5, "Configuring Content Server for IBM DB2 Database Searches."
	For information about the OCSSEARCH schema, see Section 2.2, "Creating Oracle WebCenter Content Schemas with the Repository Creation Utility."

4.3.3 Enabling or Disabling Components

You can use the Advanced Component Manager to enable or disable components.

To enable or disable components:

1. Click **Administration** on the portal navigation bar for your Content Server instance.

2. Click **Admin Server**.

   The Admin Server displays the Component Manager page.

3. In the first paragraph of the Component Manager page, click **advanced component manager**.

4. You can select individual components in this lists of enabled and disabled server components to view details about each component, and you can select categories of components to view. You can enable and disable components on this page, plus install and deinstall custom components.

   > **Note:** If you are using Records Management with Content Server, do not disable the ContentFolios component, which is required for access to the Records Management web interface. This component is enabled automatically when you configure the Records Management feature.
   >
   > For more information about Records Management, see Section 4.11, "Configuring Records Management in Content Server."

4.3.4 Configuring the Folders Interface

Oracle WebCenter Content Server provides a hierarchical folder interface, the Folders feature, for organizing and managing content in the repository. Content Server also provides the legacy hierarchical folder interface, Contribution Folders. Oracle recommends Folders (the `FrameworkFolders` component) as the folder interface for WebCenter Content because it resolves performance issues that occur with Contribution Folders (the `Folders_g` component) and includes other enhancements.

To use a folder interface, you need to enable either the `FrameworkFolders` component or the `Folders_g` component. You cannot have both enabled on a Content Server instance. Having both the Folders and Contribution Folders features enabled is not a supported configuration because some other features, such as the `CoreWebdav` system component, would not work correctly with both enabled. If you have both features enabled after an upgrade, you need to disable one of them.

To configure the folders interface:

1. In the Content Server **Administration** tray or menu, click **Admin Server**.

2. On the Component Manager page, select **Folders** to display the Folders category of components.

3. Select the **FrameworkFolders** component.

4. Click the **Update** button, and then click **OK** to confirm enabling the component.

5. In the first paragraph of the Component Manager page, click **advanced component manager**.

6. If **Folders_g** is in the Enabled Components box on the Advanced Component Manager page, select this component, and then click the **Disable** button.

7. Restart Content Server, as described in Section 9.3, "Restarting a Managed Server."

If you want to configure Contribution Folders instead of Folders, you can enable the `Folders_g` component and make sure that `FrameworkFolders` is disabled on the Advanced Component Manager page.

4.3.5 Configuring Content Server for IBM DB2 Database Searches

An IBM DB2 database does not support the keyword CONTAINS in search queries. The correct configuration of a Content Server instance for IBM DB2 searches requires the addition of the flag `SSUseContains=false` on the General Configuration page and a restart of Content Server.

To configure IBM DB2 database searches in Content Server:

1. Open a new browser window, and log in to Content Server as a system administrator (with the `sysmanager` role).

2. Under **Administration**, click **Admin Server**.

3. On the Content Admin Server page, click the name of a Content Server instance.

   The status page for the selected Content Server instance is displayed.

4. In the option list for the Content Server instance, click **General Configuration**.

   The General Configuration page is displayed.

5. Near the bottom of the page, add the following line to the Additional Configuration Variables box:

```
SSUseContains=false
```

6. Click **Save**.

7. Restart Content Server, as described in

4.3.6 Configuring Microsoft SQL Server to Work with WebCenter Content

Before you can use Microsoft SQL Server with WebCenter Content, you need to turn on snapshot isolation in the database. If you plan to use SQL Server for the back-end database for Imaging and Oracle SOA Suite, you also need to configure the Metadata Services (MDS) repository in the database and then create an MDS schema with Repository Creation Utility (RCU).

The prerequisite SQL Server configurations for WebCenter Content and the MDS repository follow:

1. Log in to the database with a user name that has DBA privileges and does not have multiple logins on the database.

   Multiple logins for the DBA would result in a lock error.

2. Alter the database to turn on the `ALLOW_SNAPSHOT_ISOLATION` option, with this command:

```
ALTER DATABASE dbname SET ALLOW_SNAPSHOT_ISOLATION ON
```

3. Alter the database to turn on the `READ_COMMITTED_SNAPSHOT` option, with this command:

```
ALTER DATABASE MDS SET READ_COMMITTED_SNAPSHOT ON
```

For information about creating an MDS schema with RCU, see

For more information about supported databases, see

4.4 Configuring OracleTextSearch for Content Server

If you have a license to use `OracleTextSearch` (with Oracle Database 11*g*), then you can configure it to use Oracle Text 11*g* as the primary full-text search engine for WebCenter Content. Oracle Text 11*g* offers state-of-the-art indexing capabilities and provides the underlying search capabilities for Oracle Secure Enterprise Search (Oracle SES). To search auxiliary metadata in Oracle WebCenter Content: Records with Oracle Text 11*g*, you must configure it to use `OracleTextSearch` as the search engine.

If you have a license to use Oracle SES, you can configure it for use with `OracleTextSearch` on WebCenter Content and configure Content Server to use Oracle SES as its back-end search engine. For more information, see "Oracle Secure Enterprise Search" in the *Oracle WebCenter Content System Administrator's Guide for Content Server*.

`OracleTextSearch` enables administrators to specify certain metadata fields to be optimized for the search index as well as to customize additional fields. `OracleTextSearch` also enables a fast index rebuild and index optimization.

You can set `OracleTextSearch` on the WebCenter Content postinstallation configuration page, which Figure 4–1 shows.

To configure OracleTextSearch for Content Server on the postinstallation configuration page:

1. Select **Internal** or **External** in the **FullText Search Option** field.

2. If you selected the **External** option, provide the name of the external data source in the **External DataSource** field.

For more information about these fields, see Section 4.3.2, "Configuring the Content Server Instance."

If you have Oracle Database 11*g*, and you specify **Internal** for **Fulltext Search Option**, you do not need to run the Repository Creation Utility (RCU) to create a search schema.

You might want to use an external data source so you can put the search engine on another system or in another database. Before you can use an external data source with `OracleTextSearch`, you need to create a search schema in a database other than the system database and configure the data source.

To create a search schema and configure an external data source:

1. Run RCU to create a search schema (*prefix*_OCSSEARCH in the database where you want the search engine, as described in Section 2.2, "Creating Oracle WebCenter Content Schemas with the Repository Creation Utility."

2. Create a JDBC data source that points to the search schema.

   You can use the Administration Console, WebLogic Scripting Tool Command, or Fusion Middleware Control to create a data source.

3. Use the Administration Console to target the data source to the WebCenter Content Managed Server (`UCM_server1` by default).

For information about creating an external data source and targeting it to a Managed Server, see "How to Create a JDBC Data Source for Oracle WebLogic Server" in the *Oracle Fusion Middleware Java EE Developer's Guide for Oracle Application Development Framework*.

If you did not configure `OracleTextSearch` on the configuration page for Content Server or you want to change the configuration, you can configure this search option in the *DomainHome*/ucm/cs/config/config.cfg configuration file for the Content Server instance. After changing the search option, you need to restart Content Server and rebuild the search index.

To configure OracleTextSearch for Content Server in the configuration file:

1. Open the *DomainHome*/ucm/cs/config/config.cfg file for the Content Server instance in a text editor.

2. Set the following values:

```
SearchIndexerEngineName=OracleTextSearch

IndexerDatabaseProviderName=SystemDatabase
```

> **Notes:**
>
> - You can specify a separate Oracle Database as the value of `IndexerDatabaseProviderName`, instead of `SystemDatabase`. The driver jar `ojdbc6.jar` is provided by Oracle in the *MW_HOME*`/wlserver_10.3/server/lib` directory. Before `Oracle Text Search` can function properly with the separate Oracle Database, however, you need to manually copy the `ojdbc6.jar` file from the *MW_HOME*`/wlserver_10.3/server/lib` directory to the *DomainHome*`/lib` directory.
>
> - `OracleTextSearch` requires a JDBC driver version of 10.2.0.4 or higher. The component will not work with older JDBC driver versions.

3. Save the file.

4. Restart Content Server, as described in Section 9.3, "Restarting a Managed Server."

5. Rebuild the search index using the **Indexer** tab of the **Repository Manager**, located under **Administration**, in **Admin Applets**.

   For more information about rebuilding the index, see "Working with the Search Index" in the *Oracle WebCenter Content System Administrator's Guide for Content Server*.

4.4.1 Applying Patches for Using Oracle Text 11g with Oracle Database 11.1.0.7.0

If you are using Oracle Database 11.1.0.7.0, you should apply the following patches to the database to prevent problems with using Oracle Text 11*g*:

- Patch 7446163

- Patch 6851110

To apply patches for using Oracle Text 11g with Oracle Database 11.1.0.7.0

1. Download patches 7446163 and 6851110 and print or save their Read Me documents from the My Oracle Support (formerly Oracle*MetaLink*) web site at

   http://support.oracle.com

2. To apply each patch, follow the instructions in its `Read Me` document.

4.4.2 Configuring an External Database Provider for Standalone Applications

You can create an external database provider in Content Server for standalone applications, such as the Batch Loader utility, to connect directly to the database with JDBC without using the SystemDatabase Provider for the Oracle WebLogic Server data source. For standalone applications to use `OracleTextSearch`, you must configure the external database provider to include the JDBC connection information.

By default, the configuration of an incoming provider does not include values for **JDBC Driver** and **JDBC Connection String**. You need to add these values, but be careful not to change the provider name because you cannot rename an existing provider. To change the name of a provider, you need to delete it and add it again. For information about changing the configuration of a provider, see "Editing Provider

Information" in the *Oracle WebCenter Content System Administrator's Guide for Content Server*.

4.5 Configuring a JDBC Driver for Standalone Applications

For Content Server to work with standalone applications, such as the Batch Loader Utility, you need to configure a JDBC driver for the system database or an external database provider. Oracle Fusion Middleware provides DataDirect JDBC drivers for Microsoft SQL Server and IBM DB2 databases to support Content Server standalone applications. You can use the System Properties utility, which Figure 4–2 shows, to enter the configuration information.

Figure 4–2 System Properties Utility
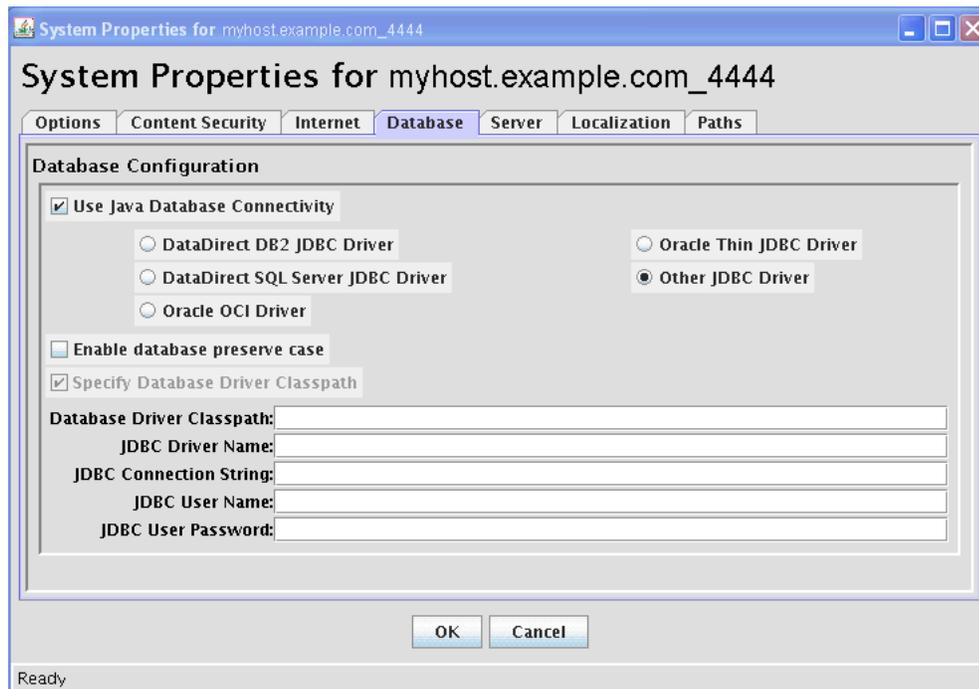
To configure a JDBC Driver for standalone applications:

1. As a system administrator, run `SystemProperties` from the `bin` directory for the Content Server instance to start the System Properties utility.

   - **UNIX path:** *DomainHome*`/ucm/cs/bin/SystemProperties`

   - **Windows path:** *DomainHome*`\ucm\cs\bin\SystemProperties`

2. On the System Properties screen, click the **Database** tab, where you can select the appropriate driver and enter the connection string, user name, and password.

   You do not need to enter a class path or driver name, or copy any JAR files.

   You can find the JDBC connection string and user name in the Oracle WebLogic Server Administration Console. Log in to the Administration Console, and then select **Services**, then **Data Sources**, then **CSDS** (or **URMDS**), and then **Connection Pool**. On the **Connection Pool** tab, the connection string is in the **URL** field, and the user name is in the **Properties** field. For security, the password is not displayed.

3. On the **Database** tab, select the appropriate driver under **Use Java Database Connectivity**, and enter the connection string.

   For Microsoft SQL Server, select **DataDirect SQL Server JDBC Driver**, and enter a connection string of this form:

   ```
   jdbc:weblogic:sqlserver://database_hostname:database_port_
   number;databaseName=database_name
   ```

   For IBM DB2, select **DataDirect DB2 JDBC Driver**, and enter a connection string of this form:

   ```
   jdbc:weblogic:db2://database_hostname:database_port_
   number;databaseName=database_name
   ```

4. Enter the user name and password for the database in the **JDBC User Name** and **JDBC User Password** fields.

5. Click **OK**.

6. Restart Content Server, as described in Section 9.3, "Restarting a Managed Server."

4.6 Importing a Database Root CA Certificate into the Key Store for a Standalone Application

Content Server components that are standalone applications do not use Oracle WebLogic Server data sources to connect and interact with a relational database management system. Standalone applications connect directly to a database using a JDBC driver.

If a standalone application is required to connect to an SSL-enabled database where digital certificates are used for authentication, then the database root CA certificate must be imported into the standard Java key store that the application uses to check trusted sources.

To import a database root CA certificate into the key store for a standalone application:

1. Import the certificate into the standard Java key store that corresponds to the application's JDK.

   The following example shows the commands to import a certificate for an application that uses the Oracle JRockit JDK on a Windows operating system:

   ```
   c:\mw_home\jrockit_160_29_D1.2.0-10\bin\keytool -import -trustcacerts
     -alias dbroot -keystore
   c:\mw_home\jrockit_160_29_D1.2.0-10\jre\lib\security\cacerts -storepass
     changeit -file b64certificate.txt
   ```

2. Configure `SystemProperties` with the SSL connection string.

   For example:

   ```
   jdbc:oracle:thin:@(
   DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCPS)(HOST=mydbhost.example.com)
   (PORT=2490
   )))(CONNECT_DATA=(SERVICE_NAME=orcl.example.com))(SECURITY=(SSL_SERVER_CERT_
   DN="CN=orcl,O=server_test,C=US")))
   ```

   For Oracle Database, you can find the SSL connection string in `tnsnames.ora`.

3. Do any other configuration required for your application, and then log in.

4.7 Enabling and Configuring Site Studio on Content Server

Before you can use Site Studio, you need to complete some configuration steps in Content Server. You can configure Site Studio on Content Server after you install the Oracle WebCenter Content software. Site Studio is available in two versions:

- **Site Studio**, which uses Site Studio Designer to create web sites

  This version requires that the SiteStudio component be enabled on Content Server. For more information, see Section 4.7.1, "Enabling Site Studio on Content Server."

  You can download the Site Studio Designer Installer from the **My Content Server** tray or menu, under **My Downloads**. For information about using this application, see the *Oracle WebCenter Content User's Guide for Site Studio Designer*.

- **Site Studio for External Applications**, which uses Oracle JDeveloper as the development environment to create Site Studio web sites

  This version requires that both the SiteStudio component and SiteStudioExternalApplications component be enabled in Content Server and both the RIDC extension and Site Studio for External Applications extension be installed on Oracle JDeveloper. For installation instructions, see "Installing Site Studio for External Applications" in the *Oracle WebCenter Content Developer's Guide for Site Studio for External Applications*. For information about using the Site Studio for External Applications extension in Oracle JDeveloper, see the Oracle JDeveloper help.

  The Remote Intradoc Client (RIDC) extension and Site Studio for External Applications extension for Oracle JDeveloper are included in the RIDC suite distribution and Web Content Management (WCM) suite distribution, respectively, which can be downloaded from the Oracle Fusion Middleware WebCenter Content section of the Oracle Technology Network (OTN) at

  http://www.oracle.com/technetwork/index.html

  If you plan to use dynamic conversion of native documents on your Site Studio web sites, then you must configure Dynamic Converter in Content Server.

The Site Studio version and Site Studio for External Applications version must have exactly the same feature extensions number; otherwise, error messages are reported and the Site Studio features will not work.

To configure Site Studio, you need to complete these tasks:

- Enabling Site Studio on Content Server

- Setting Default Project Document Information

- Setting Default Metadata for Web Site Assets

- Configuring Zone Fields

- Enabling JavaServer Pages on Content Server

- Rebuilding the Content Server Index

After you configure Site Studio, you can use Site Studio for External Applications in Oracle JDeveloper to create Site Studio web sites.

You can create an 11*g* Site Studio site running on Oracle WebLogic Server and use an Oracle Universal Content Management (Oracle UCM) 10*g*R3 server as the back end. For information about using Site Studio 11*g*R1 (11.1.1.6.0) with Oracle UCM 10*g*R3, see "Configuring Oracle Content Server 10gR3 for Use with Site Studio 11gR1" in the *Oracle WebCenter Content Technical Reference Guide for Site Studio*.

4.7.1 Enabling Site Studio on Content Server

Before you can use Site Studio, you must enable the Site Studio features on Content Server.

To enable Site Studio on Content Server:

1. Log in to WebCenter Content as an administrator.

2. In the Content Server **Administration** tray or menu, click **Admin Server**.

3. On the WebCenter Content Admin Server page, choose **Component Manager** from the **Options** list.

4. On the Component Manager page, under Web Content Management, select **SiteStudio**, **SiteStudioExternalApplications**, and **DBSearchContainsOpSupport**, and click **Update**.

   You need to enable the **SiteStudioExternalApplications** feature only if you want to use the Site Studio extension in Oracle JDeveloper.

5. Click **OK** to enable these features.

6. Restart Content Server, as described in Section 9.3, "Restarting a Managed Server."

4.7.2 Setting Default Project Document Information

When you create a new web site in Site Studio, a new project file is created and checked into Content Server for you. Before you can create web sites, you must specify the metadata that will be assigned to the new project files. You do this on the Set Default Project Document Information page in Content Server.

To set the default project document information:

1. Log in to Content Server as an administrator.

2. Go to the Administration page, and click **Site Studio Administration**.

   The Site Studio Administration page is displayed.

3. Click **Set Default Project Document Information**.

   This option displays the Set Default Project Document Information page, where you can assign the default metadata for new projects generated by Site Studio.

4. Set the metadata as required, and click **Update** when you have finished.

   This button returns you to the Site Studio Administration page.

4.7.3 Setting Default Metadata for Web Site Assets

Site Studio web sites created by Site Studio for External Applications in Oracle JDeveloper need their default metadata set in Content Server. You can set this default metadata on the Set Default Web Asset Document Information page, available through the Content Server **Administration** tray or menu under **Site Studio Administration**.

For information about setting default metadata for Site Studio web site assets, see "Set Default Web Asset Document Information Page" in the *Oracle WebCenter Content Administrator and Manager's Guide for Site Studio*.

4.7.4 Configuring Zone Fields

The Site Studio component uses several metadata fields that are added to Content Server. If you do not use `OracleTextSearch`, some of these fields must be configured as zone fields to ensure that they are full-text indexed.

Make sure that the `DBSearchContainsOpSupport` component is enabled on Content Server. This component ensures that the zone fields are full-text indexed, which is required for Site Studio sites to work correctly. If this component is not enabled, you should enable it with the Component Manager, as described in Section 4.7, "Enabling and Configuring Site Studio on Content Server."

Configuring zone fields is configuring Site Studio metadata fields as zone fields. Make sure that the zone fields are configured as follows.

To configure Site Studio metadata fields as zone fields:

1. Log in to WebCenter Content as an administrator.

2. In the Content Server **Administration** tray, click **Zone Fields Configuration**.

3. On the Zone Fields Configuration page, select **Web Sites** and **Exclude From Lists** as zone text fields.

You do not need to rebuild the search index after enabling these fields as zone fields.

4.7.5 Enabling JavaServer Pages on Content Server

If you plan to use JavaServer Pages in Site Studio, you must enable JSP on Content Server. This enables you to access and modify content and services (personalization, security definitions, predefined variables, and so on) on Content Server.

> **Important:**
>
> - JSP is supported only in legacy Site Studio projects; that is, projects that use the pre-10*g*R4 architecture. These are typically projects that were created in a Site Studio release before 10*g*R4 and that are opened in Designer 11*g*R1.
>
> - You cannot enable JSP on Content Server and then use Site Studio for External Applications remote templates in the same security group. If you did, Content Server would attempt to evaluate the Site Studio for External Applications page templates, resulting in an error that would shut down the server.

If you enable any JSP groups after you enable the Site Studio component, you must configure the JSP support so that the JSP fragments function properly.

If you enable the Site Studio component and then add a group to the list of JSP Enabled Groups in Content Server, you must redeploy the JSP support files for that group to enable Site Studio JSP fragments to work correctly.

For more information about enabling JavaServer Pages, see *Getting Started with the Software Developer's Kit (SDK)*, which is part of the Oracle Content Server 10*g*R3 documentation set.

To configure JSP Support for a new JSP group:

1. Log in to WebCenter Content as an administrator.

2. In the **Administration** tray, click **Site Studio Administration**.

3. On the Site Studio Administration page, click **Manage Fragment Libraries**.

4. Click the **Configure JSP Support** button.

    The JSP support files are extracted to the required directories on Content Server.

4.7.6 Rebuilding the Content Server Index

If you are using database search and indexing (full-text or metadata-only), you do not need to rebuild the search index after you install or upgrade the Site Studio component on Content Server. If you are using a different search engine (typically, Verity), you must rebuild the search index when installing or upgrading the Site Studio component. You should rebuild the search index after enabling the component and configuring Content Server.

The index rebuild is necessary to take advantage of new metadata fields introduced by Site Studio.

> **Important:** Rebuilding the search index can be a time-consuming process, depending on the number of content items managed by your Content Server instance. You should perform this rebuild during off-peak hours of Content Server use (typically at night or on the weekend).

If you plan to upgrade web sites created in Site Studio releases before 7.5 (see the *Oracle WebCenter Content Technical Reference Guide for Site Studio*), you must rebuild the search index on Content Server at that time. To prevent rebuilding the index more than once, you may want to skip this step until after you have successfully upgraded your sites.

For more information on rebuilding the index, see "Working with the Search Index" in the *Oracle WebCenter Content System Administrator's Guide for Content Server*.

4.8 Configuring Content Server for Desktop

Before clients can use Oracle WebCenter Content: Desktop with Content Server, you need to make sure the `CoreWebdav` system component is enabled, and you need to enable these components:

- `DesktopIntegrationSuite`

- `DesktopTag`

- `FolderStructureArchive`

- `FrameworkFolders`

You can also enable `EmailMetadata`, which maps email message fields to email metadata fields.

When you enable the `FrameworkFolders` component (Folders feature), you need to make sure that the `Folders_g` component (Contribution Folders feature) is disabled because `CoreWebdav` would not work correctly with both enabled. For more information, see Section 4.3.4, "Configuring the Folders Interface."

To configure Content Server for Desktop:

1. In the Content Server **Administration** tray or menu, click **Admin Server**.

2. On the Component Manager page, select **Folders** to display the Folders category of components.

3. Select the **FrameworkFolders** component.

4. Select the **DesktopIntegrationSuite**, **DesktopTag**, and optionally, the **EmailMetadata** components.

5. Click the **Update** button, and then click **OK** to confirm your selections.

6. In the first paragraph of the Component Manager page, click **advanced component manager**.

7. In the Disabled Components box on the Advanced Component Manager page, select **FolderStructureArchive**, and click the **Enable** button.

8. If **Folders_g** is in the Enabled Components box, select this component, and click the **Disable** button.

9. Make sure that the `CoreWebdav` component is enabled:

   a. Under Category Filters on the Advanced Component Manager page, select **Show System Components**.

   b. If **CoreWebdav** is not in the Enabled Components box, select **CoreWebdav** in the Disabled Components box, and click the **Enable** button.

10. Restart Content Server, as described in Section 9.3, "Restarting a Managed Server."

4.9 Installing and Configuring Desktop on a Client Workstation

Oracle WebCenter Content: Desktop provides a set of embedded applications that help users seamlessly integrate their desktop experiences with Content Server, Oracle Content Database, or other WebDAV-based content repositories. More specifically, these applications provide convenient access to these content repositories directly from Microsoft Windows Explorer, Microsoft Office applications (Word, Excel, and PowerPoint), and supported email clients (Microsoft Outlook and Lotus Notes).

For information about how to install Desktop on a client workstation, see "Setting Up the Desktop Client Software on Your Computer" in the *Oracle WebCenter Content User's Guide for Desktop*.

4.10 Opening Files from Microsoft Office 2010 Over a Non-SSL Connection

By default, Microsoft Office 2010 will not open files over WebDAV using basic authentication over a non-SSL connection. To get around this, you can create the following registry entry and set its value to 2:

```
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Internet\BasicAuthLevel
```
For more information, see Microsoft Knowledge Base article 2123563 on the Microsoft Support web site at

http://support.microsoft.com/kb/2123563

4.11 Configuring Records Management in Content Server

If you are licensed to configure Records Management in a WebCenter Content Managed Server, you can configure either standalone Records Management or the Oracle URM Adapter in Content Server after the Oracle WebCenter Content: Records Managed Server is configured.

> **Notes:** The `ContentFolios` component is required for access to the Records Management web interface. This component is enabled automatically when you configure Records Management in Content Server. Do not disable the `ContentFolios` component.

If you do not want to use Records Management in Content Server, you can remove the configuration user interface by disabling the `RMFeatureConfig` component. Before you disable Records Management and restart Content Server, you need to delete the Report template files that Records Management installs. You cannot delete them after Records Management is disabled. For more information about how to disable this feature, see Section 4.3.3, "Enabling or Disabling Components."

To configure Records Management in Content Server:

1. From the **Administration** tray, select **Configure Records Settings** to go to the Records Management Setup Checklist, and click **Configure Installation**.

2. On the Enabled Features page, select a Records Management option for which you are licensed:

   - **None**

   - **Standalone**

   - **Adapter**

3. Click **Submit**.

4. Restart WebCenter Content, as described in Section 9.3, "Restarting a Managed Server."

   Whenever the screen says to restart the server during the Records Management configuration, restart the WebCenter Content Managed Server.

5. After you restart WebCenter Content, the Records Management Setup Checklist is displayed again.

   For information about completing items on the Setup Checklist, see Section 8.1.2, "Completing the Setup Checklist for Records."

6. If you selected **Adapter**, click **Register Source** on the Enabled Features page, and then supply values for the fields on the Register Source page:

   - **Provider Name:** Specify the outgoing provider used to connect to the Records Managed Server. You can choose from the list of current outgoing providers, or you can click the **Add** button and create one yourself. The provider dialog box shows an abbreviated list of provider fields.

     You can also add providers from the regular Providers page. To view information about an existing provider, click **Info** in the **Action** column.

   - **Source Name:** Specify the name of the external source to be added to the Records Managed Server. The source name is required and cannot contain spaces.

- **Source Table Name:** Specify the prefix to use for creating database tables. If this value is not specified, it is defaulted to the source name.

- **Source Display Name:** Specify the caption to use for displaying the source name. If this value is not specified, it is defaulted to the source name.

After you supply the field values, click **Register**.

Before the source is actually registered, the following tests are run:

- Validate the provider and test the connection to the Records Managed Server

- Validate the specified source values

  Compare the retention schedules of the adapter and the Records Managed Server to determine whether any items in the adapter are not in the Records server. Before the source can be registered, you need to resolve any such items after on the Import Retention Schedule page. This page lists all of the items that need to be resolved and gives options for resolving the differences.

  The retention schedule needs to be synchronized between the adapter and server. By default, all of the items that need to be resolved will be imported into the Records server. You will also have the option of deleting any of the items instead of importing them into the server. Before any items are imported or deleted, backups of retention schedules are made on both the adapter and the Records server, and the backups are checked in to Content Server.

  After the source is registered, the Retention Schedule and Upload Content task will run in the background.

After the source has been successfully registered, click **OK** on the confirmation page. You will be redirected to the configuration wizard.

7. Configure the adapter on the following pages in the configuration wizard:

   - Configure Custom Fields

     The Configure Custom Fields page enables you to specify custom fields on the external source. When you add or edit custom fields, you map them to existing document metadata fields defined in Content Server. You can use the same name for each field as defined in Content Server, or you can rename the field to something different. When the content is uploaded to the Records server as external content items, these fields are mapped to their external field names.

     You can configure custom fields, as needed, in any of these ways:

     * Add an external custom field.

     * Edit an external custom field.

     * Configure the disposition actions.

     * Configure the scheduled events.

     * View the external source information (from the **Info** menu, select **Source Information**).

   - Configure Scheduled Times

     The Configure Scheduled Times page enables you to specify when the scheduled tasks are to run. You can specify the interval at which the tasks are run (in hours, days, or weeks) and the time of day. This enables you to schedule the tasks at times when there might be less activity.

8. After Records Management is initially configured on Content Server, the menu bar includes a **Records** menu. You can change the Records Management configuration through options on this menu.

   For more information about configuring Records Management, see the *Oracle WebCenter Content Setup Guide for Records*.

9. From the **Records** menu, select **Configure** and then **Enabled Features**.

   On the Enabled Features page, you can change the selection of features and dispositions. For the adapter, the features you select cannot be more than the features selected on the Records server. For more information about the Features and Disposition Actions sections of the Enabled Features page, see Section 8.1.1, "Configuring the Level of Records Features."

   After you change any features or dispositions, restart WebCenter Content, as described in Section 9.3, "Restarting a Managed Server."

4.12 Configuring Oracle Application Extension Framework

Oracle Application Extension Framework (AXF) is automatically installed with Imaging. For information about verifying the installation, see Section 6.5, "Installing and Configuring Oracle Application Extension Framework."

For information about configuring and using AXF and the AXF database tables, see the *Oracle WebCenter Administrator's Guide for Application Adapters*.

4.13 Installing and Configuring Oracle Document Capture and Oracle Distributed Document Capture

Oracle Document Capture provides high-volume production scanning from a central location, while Oracle Distributed Document Capture provides a user-friendly web interface that enables distributed enterprises to capture images easily from remote locations.

For information about installing and configuring Oracle Document Capture, see the *Oracle Document Capture Installation Guide* and the *Oracle Document Capture Administrator's Guide*.

For information about installing and configuring Oracle Distributed Document Capture, see the *Oracle Distributed Document Capture Installation Guide* and the *Oracle Distributed Document Capture Administrator's Guide*.

The WebCenter Content 11*g* Commit Driver is required to commit documents from either capture application to WebCenter Content. For information about using the WebCenter Content 11*g* Commit Driver, see the *Oracle Distributed Document Capture Installation Guide* or the *Oracle Distributed Document Capture Administrator's Guide*.

5

Completing the Inbound Refinery Configuration

This chapter explains how to complete the initial configuration of Oracle WebCenter Content: Inbound Refinery in an Oracle WebLogic Server domain.

This chapter includes the following sections:

- Section 5.1, "Completing the Initial Inbound Refinery Configuration"
- Section 5.2, "Installing and Configuring Inbound Refinery on WebCenter Content"

5.1 Completing the Initial Inbound Refinery Configuration

Before you can use Inbound Refinery with Oracle WebCenter Content, you need to complete the configuration of Inbound Refinery for document and image conversions to work with Content Server.

For transformations to work on some platforms, certain environment variables must be set before you start the Managed Server. On a UNIX operating system running XWindows, to redirect the display to a system with suitable graphic capabilities, you need to export DISPLAY to a valid X Server before starting the Inbound Refinery Managed Server. For more information, see Section 3.7.2, "Setting Library Paths in Environment Variables on UNIX Platforms."

To complete the Inbound Refinery configuration:

1. Start the Administration Server and the Inbound Refinery and WebCenter Content Managed Servers, as described in Chapter 9, "Verifying the Oracle WebCenter Content Configuration."

2. Configure Content Server, as described in Section 4.2, "Completing the Initial WebCenter Content Configuration."

3. Browse to the Inbound Refinery postinstallation configuration page, at this web site:

   ```
   http://managedServerHost:16250/ibr/
   ```

4. Enter or edit all necessary values.

   - To enable access from Content Server, provide a value for **Incoming Socket Connection Address Security Filter**, as follows:

     ```
     127.0.0.1|0:0:0:0:0:0:0:1|your.server.IP.address
     ```

This value should be the IP address of the Content Server instance or instances that will send jobs to Inbound Refinery, not the IP address of Inbound Refinery. (In a test or demo environment, these IP addresses could be the same.)

This field accepts wildcards in the value, like `10.*.*.*`. You can change this value later by setting `SocketHostAddressSecurityFilter` in *DomainHome*/ucm/ibr/config/config.cfg and restarting Inbound Refinery.

Note: The **Incoming Socket Connection Address Security Filter** value must be set correctly for Inbound Refinery to be usable.

- In the **Server Socket Port** field, if you want to set up a provider from Inbound Refinery back to Content Server, enter an unused port number, such as `4444`, for Server Socket Port.

  This value is the number of the port for calling top-level services. Changing this field value changes the `IntradocServerPort` entry in *DomainHome*/ucm/ibr/config/config.cfg.

Note: The **Server Socket Port** value must be set correctly for Inbound Refinery to be usable.

---

5. Restart Inbound Refinery, as described in Section 9.3, "Restarting a Managed Server."

6. Check all the entries in *DomainHome*/ucm/ibr/config/config.cfg have the values that you want for the Inbound Refinery configuration.

5.2 Installing and Configuring Inbound Refinery on WebCenter Content

Inbound Refinery is a conversion server that manages file conversions for electronic assets such as documents, digital images, and motion video. In addition to conversion, Inbound Refinery provides thumbnail functionality for documents and images, storyboarding for video, and the ability to extract and use EXIF data from digital images and XMP data from electronic files generated from programs such as Adobe Photoshop and Adobe Illustrator. You can use Inbound Refinery to convert content items stored in Content Server.

The installation and configuration of Oracle WebCenter Content includes Inbound Refinery. Before you can use Inbound Refinery with WebCenter Content, you need to complete the configuration for document and image conversion to work with Content Server. To complete the configuration, perform these tasks:

- Configuring Inbound Refinery on WebCenter Content

- Configuring Document Conversion on Inbound Refinery

- Setting Up Content Server to Send Jobs to Inbound Refinery for Conversion

- Changing the Path to the Font Directory for Inbound Refinery (Optional)

5.2.1 Configuring Inbound Refinery on WebCenter Content

Inbound Refinery has a postinstallation configuration page that you need to complete after the configuration of Content Server.

To configure Inbound Refinery on WebCenter Content:

1. Configure Content Server, as described in Section 4.3, "Completing the Initial Configuration of Content Server."

2. Browse to the Inbound Refinery postinstallation configuration page, at this web site:

   `http://managedServerHost:16250/ibr/`

   Figure 5–1 shows the Inbound Refinery Configuration page for postinstallation configuration.

Figure 5–1   Inbound Refinery Configuration Page

3. Enter or edit all necessary values.

   The following table describes the field values on the Inbound Refinery Configuration page, where the required values are marked with asterisks, as Figure 5–1 shows.

Field	Description
Inbound Refinery Instance Folder	The absolute path to the Oracle instance directory of Inbound Refinery, which is *DomainHome*/ucm/by default.
	The default Oracle instance directory for Inbound Refinery follows:
	`MW_HOME/user_projects/domains/`*DomainHome*`/ucm/ibr`
	The name of the top-level folder in the folder hierarchy for the Content Server instance is `ibr`.
	The path to the Oracle instance directory is the value of the `IntradocDir` variable for the Inbound Refinery instance. This directory path should be unique to this particular Managed Server, or node. For installations that are likely to be upgraded to future versions of the product, Oracle strongly recommends that you change the location of the Oracle instance directory to a directory outside of any Oracle WebLogic Server domain directories or installation directories.
Native File Repository Location	The directory where conversion jobs are stored while they are being processed. After a job is converted and picked up by Content Server, the job is removed from this directory. You do not need to change this path.
Weblayout Folder	The URL for the Inbound Refinery web interface. You do not need to change this path.
Register Start Menu Actions	Whether or not the **Start Menu** actions will be registered.
Server Socket Port	The number of the port for calling top-level services.
	To set up a provider from Inbound Refinery back to Content Server, you can leave the default **Server Socket Port** value, `5555`, or change it to an unused port number.
	Changing this field value changes the `IntradocServerPort` entry in *DomainHome*/ucm/ibr/config/config.cfg.
	Note: The **Server Socket Port** value must be set correctly for Inbound Refinery to be usable.
Incoming Socket Connection Address Security Filter	Restricts Inbound Refinery access to a computer or computers with a specified IP address or addresses.
	To enable access from Content Server, provide a value for this field as follows:
	`127.0.0.1|0:0:0:0:0:0:0:1|`*your.server.IP.address*
	This value should be the IP address of the Content Server instance or instances that will send jobs to Inbound Refinery, not the IP address of Inbound Refinery. (In a test or demo environment, these IP addresses could be the same.)
	This field accepts wildcards in the value, like `10.*.*.*`. You can change this value later by setting `SocketHostAddressSecurityFilter` in *DomainHome*/ucm/ibr/config/config.cfg and restarting Inbound Refinery.
	Note: The **Incoming Socket Connection Address Security Filter** value must be set correctly for Inbound Refinery to be usable.
Web Server HTTP/HTTPS Address	The name of the web server. (`HttpServerAddress` property).

Field	Description
Web Address Is HTTPS	Whether or not the URL for the web server starts with `HTTPS`, for a server that has SSL enabled.
Inbound Refinery URL Prefix	The relative URL for the Inbound Refinery instance.
Server Instance Name	The name of the Inbound Refinery instance.
Server Instance Label	The instance name that is displayed for Inbound Refinery.
Server Instance Description	A description of the Inbound Refinery instance.

4. Restart Inbound Refinery, as described in Section 9.3, "Restarting a Managed Server."

5. Restart Content Server.

You can restart a Content Server instance by restarting the WebCenter Content Managed Server, with the Oracle WebLogic Server Administration Console, shutdown and startup scripts, or Oracle Enterprise Manager Fusion Middleware Control. For more information, see Section 9.3, "Restarting a Managed Server."

After you restart the WebCenter Content Managed Server, you can set up Inbound Refinery and Content Server for document conversion. The core Inbound Refinery uses Outside In technology to convert native documents to web-viewable PDF files or JPEG thumbnails. Other conversions require additional Inbound Refinery components. These components are installed but disabled on Inbound Refinery by default. Some of these components are only for running on Windows operating systems, some require additional configuration, and some require certain components to be enabled on Content Server.

For Inbound Refinery to work properly, it must have access to the fonts it needs to generate images. By default, the font path is set to the font directory in the JDK used by Inbound Refinery: `java.home/lib/fonts`. However, the fonts included in the default directory are limited and might cause poor renditions. Also, if a nonstandard JDK is used, then the JDK font path may be different than that specified as the default. In these cases, you might need to change the font path to improve the quality of the renditions or to provide the correct path to the font directory in the JDK. For more information, see Section 5.2.4, "Changing the Path to the Font Directory for Inbound Refinery."

On Content Server, you must set up an outgoing provider from Content Server to Inbound Refinery, with the **Handles Inbound Refinery Conversion Jobs** option checked, as described in Section 5.2.3.1, "Creating an Outgoing Provider." You also need to enable any components that you need for your conversion types. The `InboundRefinerySupport` component is enabled by default on a new Content Server instance. If this component is not enabled, you must enable it on any Content Server instance that will use Inbound Refinery for document conversion, as described in Section 5.2.2.1, "Enabling Conversion Components on Inbound Refinery."

5.2.2 Configuring Document Conversion on Inbound Refinery

To configure document conversion on Inbound Refinery, perform these tasks:

- Enabling Conversion Components on Inbound Refinery
- Enabling PDFExportConverter in Inbound Refinery

5.2.2.1 Enabling Conversion Components on Inbound Refinery

The core Inbound Refinery converts files to TIFF web-viewable files and JPEG image thumbnails. To use additional conversion types, you will need to enable the necessary components.

For information about the conversion components, see "Inbound Refinery Conversion Options and Related Components" in the *Oracle WebCenter Content Administrator's Guide for Conversion*.

To enable conversion components on Inbound Refinery:

1. From the Inbound Refinery **Administration** menu, select **Admin Server** and then **Server Features**.

2. Select the components you want.

3. Click **Update**.

4. Click **OK** to enable the components.

5. Restart Inbound Refinery, as described in Section 9.3, "Restarting a Managed Server."

For more information, consult the readme files and the documentation for each component.

5.2.2.2 Enabling PDFExportConverter in Inbound Refinery

PDFExportConverter uses Outside In to convert documents directly to PDF files. The conversion can be cross-platform and does not require any third-party product. You can enable PDFExportConverter for Inbound Refinery as a server feature.

To enable PDFExportConverter on Inbound Refinery:

1. From the Inbound Refinery **Administration** menu, select **Admin Server** and then **Server Features**.

2. Select **PDFExportConverter**, and click the **Update** button.

3. Click **Update**.

4. Click **OK** to enable this feature.

5. Restart Inbound Refinery, as described in Section 9.3, "Restarting a Managed Server."

6. Set the primary web-viewable conversion to PDF Export.

   For more information, see "Setting PDF Files as the Primary Web-Viewable Rendition" in the *Oracle WebCenter Content Administrator's Guide for Conversion*.

7. Make sure that file formats are configured on Content Server to be sent to Inbound Refinery, as described in Section 5.2.3.3, "Selecting File Formats To Be Converted."

5.2.3 Setting Up Content Server to Send Jobs to Inbound Refinery for Conversion

Before Content Server can send jobs to Inbound Refinery for conversion, you need to perform these setup tasks:

- Creating an Outgoing Provider

- Enabling Components for Inbound Refinery on Content Server

- Selecting File Formats To Be Converted

5.2.3.1 Creating an Outgoing Provider

Before Content Server can send files to Inbound Refinery for conversion, you must set up an outgoing provider from Content Server to Inbound Refinery with the **Handles Inbound Refinery Conversion Jobs** option checked.

To create an outgoing provider:

1. From the Content Server **Administration** menu, choose **Providers**.

2. In the Create a New Provider section of the Providers page, click **Add** in the **outgoing** row.

3. Enter values for these fields:

    -   **Provider Name:** Any short name with no spaces. It is a good idea to use the same value as the **Instance Name** value

    -   **Provider Description:** Any text string.

    -   **Server Host Name:** The name of the host machine where the Inbound Refinery instance is running, such as `myhost.us.example.com:16250`.

    -   **HTTP Server Address:** The address of the Inbound Refinery instance, such as `myhost.example.com:16250`.

    -   **Server Port:** The value that was entered in the **Server Socket Port** field (`IntradocServerPort` value) for the Inbound Refinery instance. This value is the number of the port for calling top-level services.

        You can find this value on the Inbound Refinery configuration information page, as follows:

        a. From the Inbound Refinery **Administration** menu, select **Configuration Information**.

        b. Next to **Server Name**, click **Server Configurations**.

        c. Look for the value for **Server Port**.

    -   **Instance Name:** The instance name for Inbound Refinery (the `IDC_Name` value in the **config.cfg** file).

        This value was entered on the postinstallation configuration page for **Server Instance Name**.

        You can also find this value on the Inbound Refinery configuration information page, as follows:

        a. From the Inbound Refinery **Administration** menu, select **Configuration Information**.

        b. Look for the **Server Name**, value.

    -   **Relative Web Root**: The web root of the Inbound Refinery instance, `/ibr/`.

4. Under Conversion Options, check **Handles Inbound Refinery Conversion Jobs.**

    Do *not* check **Inbound Refinery Read Only Mode**.

5. Click **Add**.

6. Restart Content Server, as described in Section 9.3, "Restarting a Managed Server."

7. Go back to the Providers page, and check that the **Connection State** value is `good` for the provider.

If the value is not `good`, double-check that you entered all the preceding entries correctly, and check that the Content Server and Inbound Refinery instances can ping each other.

For more information about setting up providers, see "Configuring Content Server and Refinery Communication" in the *Oracle WebCenter Content Administrator's Guide for Conversion*.

5.2.3.2 Enabling Components for Inbound Refinery on Content Server

Some conversion types require *helper* components to be enabled on Content Server. The `InboundRefinerySupport` component must always be enabled on any Content Server instance that uses Inbound Refinery for document conversion. It is enabled by default on a new Content Server installation.

To enable components for Inbound Refinery on Content Server:

1. From the Content Server **Administration** menu, choose **Admin Server** and then **Component Manager**.

2. Under Inbound Refinery, select the components that you want to enable.

3. Click **Update**.

4. Restart Content Server, as described in Section 9.3, "Restarting a Managed Server."

5.2.3.3 Selecting File Formats To Be Converted

To tell Content Server which files to send to Inbound Refinery to be converted, you need to select file formats.

To select file formats to be converted:

1. From the Content Server **Administration** menu, choose **Refinery Administration** and then **File Formats Wizard**.

    Content Server displays the File Formats Wizard page. This page configures what file formats will be sent to Inbound Refinery for conversion when they are checked into Content Server.

2. Select the formats you want converted.

3. Click **Update**.

You can also select file formats with the Configuration Manager, with more fine-grained control, including file formats that wizard does not list. For more information, see "Using the File Formats Wizard" and "Using the Configuration Manager" in the *Oracle WebCenter Content Administrator's Guide for Conversion*.

5.2.4 Changing the Path to the Font Directory for Inbound Refinery

The default font path for Inbound Refinery is the font directory in the JVM, `java.home/lib/fonts`. You might need to change the path, in some cases, to improve the quality of renditions or to specify the correct path to the font directory in a nonstandard JDK.

If the JDK font path is different from the default font path, an error message is displayed from both Inbound Refinery and Content Server. If you receive an error message, ensure that the font path is set to the directory containing the fonts necessary to properly render your conversions. If the native file contains custom fonts or non-western European characters, Inbound Refinery must have access to these fonts.

To change the path to the font directory for Inbound Refinery:

1. Log in to Inbound Refinery.

2. From the **Administration** tray or menu, choose **Conversion Settings**, then **Third-Party Application Settings**.

3. Click **Options** under General OutsideIn Filter Options.

4. Replace the path to the font directory on the General OutsideIn Filter Option page.

5. Click **Update**.

6

Completing the Imaging Configuration

This chapter explains how to complete the initial configuration of Oracle WebCenter Content: Imaging in an Oracle WebLogic Server domain.

This chapter includes the following sections:

- Section 6.1, "Completing the Initial Imaging Configuration"
- Section 6.2, "Configuring the Full-Text Features in the WebCenter Content Repository"
- Section 6.3, "Connecting to a Workflow Server"
- Section 6.4, "Setting Imaging System Security"
- Section 6.5, "Installing and Configuring Oracle Application Extension Framework"
- Section 6.6, "Installing and Configuring Oracle Document Capture and Oracle Distributed Document Capture"

6.1 Completing the Initial Imaging Configuration

Before you complete the configuration of Imaging, your system needs to have Oracle WebCenter Content installed and configured. Imaging uses WebCenter Content for its repository.

You can use either WebCenter Content 11*g* or Oracle Universal Content Management (Oracle UCM) 10*g*R3 as the Imaging repository. For information about configuring WebCenter Content 11*g*, see Chapter 3, "Configuring Oracle WebCenter Content Applications," Chapter 4, "Completing the WebCenter Content Configuration," and Section 6.1.1.1, "Configuring WebCenter Content 11g to Work with Imaging." For information about using Oracle UCM 10*g*R3 as the repository, see Section 6.1.1.2, "Installing and Configuring Oracle UCM 10gR3 to Work with Imaging."

> **Note:** In a production system, Oracle WebCenter Content 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 Imaging with an external LDAP authentication provider, it is easier to do this before you complete the configuration of the Imaging Managed Server and before you connect it to the WebCenter Content 11*g* or Oracle UCM 10*g*R3 repository. For more information, see Section 3.9, "Reassociating the Identity Store with an External LDAP Authentication Provider."

The user who logs in first to an Imaging Managed Server is provisioned with full security throughout the server. When this user first logs in, Imaging provides a user interface to complete the configuration, including connecting to a repository or repositories and, optionally, to a workflow server.

If a value is specified in the `DefaultSecurityGroup` MBean before Imaging security is initialized, then when the first user logs in, the specified group is given full administrative permissions as well as the user logging in.

To complete the Imaging configuration, you need to perform all of the following tasks that apply to your system:

1. Configuring a WebCenter Content Repository for Imaging

2. Starting the Administration Server and the WebCenter Content Managed Server, as described in Chapter 9, "Verifying the Oracle WebCenter Content Configuration"

3. Starting the Imaging Managed Server and Accessing the Web Client

4. Connecting to a WebCenter Content Repository

5. Configuring the GDFontPath MBean for a UNIX System

6. Setting DISPLAY for the Imaging Viewer in a UNIX Exalogic Environment with Solaris 11g

7. Importing Definitions

6.1.1 Configuring a WebCenter Content Repository for Imaging

You can configure either WebCenter Content 11*g* or Oracle UCM (Oracle Content Server) 10*g* R3 as the repository for Imaging.

> **Note:** You will not be able to import or upload content to the Imaging system unless you have created a repository connection.

6.1.1.1 Configuring WebCenter Content 11g to Work with Imaging

WebCenter Content 11*g* is installed with Oracle WebCenter Content. When a WebCenter Content Managed Server and Imaging Managed Server are configured in an Oracle WebLogic Server domain on the same host machine, the configuration of WebCenter Content 11*g* to work with Imaging is automatic.

If WebCenter Content is installed in a domain that is later extended with Imaging, then WebCenter Content will not be reconfigured to work with Imaging until the next restart of the WebCenter Content Managed Server. In this case, you must restart WebCenter Content, as described in Section 9.3, "Restarting a Managed Server," before connecting to Oracle WebCenter Content Server from the Imaging web client, as described in Section 6.1.3, "Connecting to a WebCenter Content Repository."

If the WebCenter Content and Imaging Managed Servers are configured to run on different machines, configuring Imaging will not configure WebCenter Content to work with it. In this case, you must follow the manual configuration steps to configure WebCenter Content.

To configure WebCenter Content 11g manually to work with Imaging:

1. Start the WebCenter Content Managed Server, as described in Section 9.2, "Starting Managed Servers."

2. Access Content Server, as described in Section 4.3.1, "Starting Content Server."

3. Enable the `IpmRepository` component:

   a. Choose **Admin Server** from the **Administration** tray or menu.

   b. On the Content Admin Server Component Manager page, select **Integration.**

   c. Select **IpmRepository**, and click the **Update** button.

   This option is selected by default if the Oracle WebLogic Server domain was configured with Fusion Middleware Configuration Wizard. If this option is already selected, you can close the Component Manager without clicking **Update** or restarting Content Server.

   d. Click the **OK** button to enable this feature.

   e. Restart Content Server, as described in Section 9.3, "Restarting a Managed Server."

   If **IpmRepository** was already selected, you do not need to restart the server.

6.1.1.2 Installing and Configuring Oracle UCM 10gR3 to Work with Imaging

For an Oracle UCM 10*g*R3 repository, Imaging requires Oracle Universal Content Management 10*g*R3 (10.1.3.3.3), also referred to as Oracle Content Server 10*g*R3. After installing and configuring Oracle Content Server 10*g*R3, you need to update the system with the Content Server 10*g* Update Bundle. Both are required for Oracle UCM 10*g*R3 to work with Imaging 11*g*.

You can download both Oracle Content Server 10*g*R3 and the Content Server 10*g* Update Bundle from the Oracle Software Delivery Cloud or Oracle Technology Network (OTN). For more information about the software locations, see Section 1.2.2, "Software Downloads for Oracle WebCenter Content Installation and Configuration."

For information about installing and configuring Oracle UCM 10*g*R3, see the Oracle Content Server page on Oracle Technology Network at

`http://www.oracle.com/technetwork/middleware/content-management/cs-0888`
`69.html`

If you are using Imaging 11*g* with Oracle UCM 10*g*R3, make sure to update Oracle Content Server 10*g*R3 with the latest update patch.

6.1.1.2.1 Upgrading the JDK Version of Oracle UCM 10gR3

After you deploy Imaging to an Oracle WebLogic Server Managed Server, by creating or extending a domain, you need to upgrade the JDK version of your Oracle Content Server 10*g*R3 installation to the same JDK 1.6 version that Imaging uses. This is the JDK version that you specified for the Imaging Managed Server on the Configure Server Start Mode and JDK screen of the Fusion Middleware Configuration Wizard. For information about the JDK version that Imaging supports, 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`

Refer to the Oracle Fusion Middleware 11g Release 1 (11.1.1.*x*) Product Area, **System Requirements and Supported Platforms for Imaging and WebCenter Content (xls)**.

For information about changing the JDK version that Oracle Content Server 10*g*R3 uses, see *Oracle Universal Content Management Content Server Installation Guide*, version 10*g*R3, for your operating system.

6.1.1.2.2 Configuring Oracle Content Server 10gR3 to Work with Imaging You need to configure Oracle Content Server 10*g*R3 before it can work with Imaging. During the configuration, restart Oracle Content Server 10*g*R3 whenever prompted to do so.

To configure Oracle Content Server 10gR3 to work with Imaging:

1. Update the IP address filter:

   a. On the system where Oracle UCM 10*g*R3 is installed, run the following command:

      * **UNIX command:** *UCM_ORACLE_HOME*/bin/SystemProperties

      * **Windows command:** *UCM_ORACLE_HOME*\bin\SystemProperties

   b. With your system's DISPLAY environment variable set to a valid X Server, click the **Server** tab in the display.

   c. In the **IP Address Filter** field, add a vertical bar (|) followed by the IP address of the system where Imaging is installed.

      For example: 192.0.2.1|192.0.2.130

      The IP address is required for the Imaging system to have access to the Oracle UCM 10*g*R3 system without authentication.

   d. Click **OK**.

      This change will require a restart of Oracle Content Server 10*g*R3, which you can do at the end of this procedure, after installing the Oracle UCM 10*g*R3 components.

2. Open the Oracle UCM 10*g*R3 web client in a web browser (http://*managedServerHost*:*managedServerPort*/*location*, such as http://myhost.example.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 10*g*R3 does the upgrade automatically.

   Imaging content is not accessible in a web store. Oracle Content Server 10*g*R3 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 Imaging solution and uses extra disk space. After the file store upgrade, you should disable the weblayout functionality in Oracle Content Server 10*g*R3 for any file store provider configured for use as an Imaging volume.

5. Configure system properties:

a. Confirm that the `SearchIndexerEngineName` variable matches the type of Oracle UCM 10*g*R3 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 by adding the following line to the Additional Configuration Variables box:

```
EnableIdcProfileField=1
```

h. Click **Save**.

6. Install Oracle UCM 10*g*R3 components:

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

b. In the Install New Component section, click **Browse**, browse to the `/extras` directory, and select any components you want to install.

c. Click **Open**.

d. Click **Install**.

If the Component Manager redirects your request to port 80, you can reconfigure your web server to use port 80.

Restart Oracle Content Server 10*g*R3 when prompted.

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

The menu displays several selections, some of which are checked. You can accept the default selections.

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

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

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

i. Click **Open**.

j. Click **Install**.

Restart Oracle Content Server 10*g*R3 when prompted.

k. Click **Continue**.

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

m. In the Install New Component section, click **Browse** and browse to the `/extras` directory.

n. Select any components in the `/extras` directory and **IpmRepository**.

o. Click **Enable**.

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

Restart Oracle Content Server 10*g*R3 when prompted.

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

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

s. Select **Restart**.

t. Ensure that Oracle Content Server 10gR3 is running after you restart it.

6.1.1.2.3 Adding the Administrator User and Administrators Group to Oracle UCM 10gR3 You need to add the administrator user to Oracle UCM 10*g*R3 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 10gR3:

1. In the Oracle UCM 10*g*R3 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.

6.1.1.3 Configuring a File Store Provider for Content Storage

An administrator can configure a file store provider in Content Server 11*g* to control how and where files are stored and managed within Content Server. Instead of storing all content on a single file system, you can use a file store provider to store content across multiple file systems as well as within a database. The File Store Provider component is installed and enabled by default with WebCenter Content installation and configuration.

For Imaging, you should add a file store provider to use instead of the default file store provider. Also, you should disable the traditional web layout functionality for the file store.

The default storage provider configuration that is created during the installation of WebCenter Content is not intended for production document volumes. This default configuration is adequate for proof-of-concept or demonstration systems of fewer than

10,000 documents. Production system configurations require more advanced options to be chosen.

You can configure a file store provider for Oracle Database.

If your WebCenter Content installation uses a Microsoft SQL Server or IBM DB2 database, do not configure a file store provider. If you are configuring a WebCenter Content Managed Server with one of these databases, you need to disable the file store provider that is enabled by default for Content Server.

For more information, see "Configuring a File Store System" in the *Oracle WebCenter Content System Administrator's Guide for Content Server*.

6.1.1.3.1 Configuring a File Store Provider A file store provider can be a combination of any media supported by Content Server. Because the document storage location is not defined by the media being used for storage, the term **volume** is used to represent a storage location when an application is defined in the Imaging user interface. Imaging connects to a volume defined and configured in Content Server by an administrator. You cannot use Imaging to create or define a volume.

A Content Server administrator can configure a file store provider. For more information, see "File Store Administration Interface" in the *Oracle WebCenter Content System Administrator's Guide for Content Server*.

6.1.1.3.2 Disabling Web Layout Functionality for Imaging Content Server traditionally uses a `/weblayout` directory on a file system to store content in a format for viewing in a web browser, even if the main storage volume is set up in a database. This file system store is useful for making content retrieval faster for a web site or for storing a secondary file that describes the primary content item, but it does not have much use in an Imaging solution. Files copied to a `/weblayout` directory in an exclusively Imaging solution would never get used, taking up unnecessary storage space. Oracle recommends disabling the web layout functionality for any file store provider that is configured for use as an Imaging volume.

An administrator can disable the web layout functionality by selecting the **Is Webless File Store** option on the Add/Edit Storage Rule page for a file store provider in Content Server. For more information, see "Add/Edit Storage Rule Page" in the *Oracle WebCenter Content System Administrator's Guide for Content Server*.

6.1.2 Starting the Imaging Managed Server and Accessing the Web Client

After you start the Administration server and the Imaging and WebCenter Content Managed Servers, you can access the Imaging web client.

To access the Imaging web client:

1. Start the Imaging Managed Server, as described in

2. Access the web client at this URL:
   `http://managedServerHost:16000/imaging`

   Log in with the administrator user name and password.

   > **Note:** This first user to connect to the Imaging system is registered as the Imaging administrator.

6.1.3 Connecting to a WebCenter Content Repository

Before Imaging can use the WebCenter Content repository, you need to configure a connection to Content Server. You can create a connection to it from Imaging.

To connect to a WebCenter Content repository:

1. Open a web browser, and navigate to this web site:

   `http://managedServerHost:16000/imaging`

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

3. Navigate to the **Manage Connections** tray, and choose **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. You can change the selections and on the Connection Settings page:

   ■ **SSL:** Selected for secure SSL communications

   ■ **Server Port:** The IDC port of the WebCenter Content instance, `4444` for Imaging by default

   ■ **Use Local Content Server:** Selected by default if Content Server is on the same machine as the Imaging server.

   If the servers are not installed on the same machine, you will need to configure the Content Server machine name as part of the Content Server Pool.

6. Click **Next**.

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. At least one user or group must have the grant access permission.

8. Click **Next**.

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

6.1.4 Configuring the GDFontPath MBean for a UNIX System

For conversions to work correctly on a UNIX operating system, it needs to have TrueType fonts available. If these fonts are not available on your system, you need to install them. To set the font path on a UNIX operating system, you need to configure the `GDFontpath` MBean. You can configure it through the System MBean Browser in Oracle Enterprise Manager Fusion Middleware Control.

To configure the GDFontPath MBean for a UNIX system:

1. Access the Imaging domain in 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.example.com: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 **GDFontPath** attribute to the location of your True Type Fonts (TTF) files; for example:

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

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

   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, Imaging 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 Imaging. 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 Imaging 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`

   - HP-UX Itanium: `/usr/lib/X11/fonts/TrueType`

   - Linux: `/usr/lib/X11/fonts/TrueType`

9. Click **Apply**.

10. Restart Imaging, as described in Section 9.3, "Restarting a Managed Server."

6.1.5 Setting DISPLAY for the Imaging Viewer in a UNIX Exalogic Environment with Solaris 11g

In an Exalogic environment with Solaris 11*g*, you need to set the DISPLAY environment variable for the Imaging Viewer to work correctly in basic mode.

To set DISPLAY for the Imaging Viewer in a UNIX Exalogic Environment with Solaris 11g:

1. Open a new terminal window and run this command:

   ```
   xhost +
   ```

2. In the Imaging terminal, set the DISPLAY environment variable to the server where Imaging is running and the port, in this format:

   ```
   servername:port
   ```

3. Restart Imaging, as described in Section 9.3, "Restarting a Managed Server."

6.1.6 Importing Definitions

At this point in the installation process, you can use the Import tool to import previously exported Imaging definitions (applications, searches, and inputs).

6.2 Configuring the Full-Text Features in the WebCenter Content Repository

Imaging supports two types of full-text searching under WebCenter Content: `DATABASE.FULLTEXT` and `OracleTextSearch`. Imaging can use the full-text features if you configure full-text searching in the WebCenter Content repository first. For `DATABASE.FULLTEXT` systems, after the indexes are rebuilt, nothing needs to be done on the Imaging side. `OracleTextSearch`, however, requires that the index be rebuilt any time an application with `FullText` enabled is created, deleted, or has modifications that involve field definitions.

For more information on configuring full-text searching, see Section 4.4, "Configuring OracleTextSearch for Content Server."

For additional full-text configuration options, see "Configuring the Search Index" in the *Oracle WebCenter Content System Administrator's Guide for Content Server*.

After full-text is enabled in WebCenter Content, you will need to create an application and check the `FullText` option on the application. For more information, see "Specifying General Properties" in *Oracle WebCenter Content Administrator's Guide for Imaging*.

6.3 Connecting to a Workflow Server

A connection to a workflow server will be necessary for your solution to retrieve your task list. Imaging connects to a workflow server when application fields are mapped to workflow payload elements. To connect, the provider, port, and credential information is passed using Web Services Inspection Language (WSIL). WSIL uses the HTTP protocol and a specific XML format to allow for the discovery of the web service end points on a server. Imaging follows links in the WSIL that meet certain criteria to discover deployed composites.

The connection can be to an Oracle Business Process Management (Oracle BPM) or Business Process Execution Language (BPEL) server. For Imaging to take advantage of BPM and Oracle BPEL Process Manager within an existing domain, the domain must be extended with **Oracle BPM Suite - 11.1.1.0**. When Oracle BPM Suite was installed, it automatically selected **Oracle SOA Suite - 11.1.1.0** as its dependency. If you want to use Oracle BPEL Process Manager and not Oracle BPM, you can extend the domain with an Oracle SOA Suite installation and configuration. For more information about the installation and configuration steps for Oracle SOA Suite and Oracle BPM, see *Oracle Fusion Middleware Installation Guide for Oracle SOA Suite and Oracle Business Process Management Suite*.

For more information about connecting to a workflow server, see "Creating a Workflow Connection" in *Oracle WebCenter Content Administrator's Guide for Imaging*.

After you have created a workflow connection, enter the name of that connection in the **AXF_SOLUTION_ATTRIBUTES** table for your solution. For example, the parameter key for a Business Process Execution Language (BPEL) server is named **BPEL_CONNECTION**, and the HelloBPEL sample script uses the connection name `test`.

6.4 Setting Imaging System Security

On a new Imaging 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.

> **Note:** If you configure Imaging for use with Oracle Access Manager, you must protect the `imaging/faces/` directory. Failure to do so would prevent access to the Imaging Viewer.

If security provider changes are made after this initial user login to Imaging, take the following steps to reset Imaging 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 Imaging 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 3.9, "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 Imaging database.

6.5 Installing and Configuring Oracle Application Extension Framework

Oracle Application Extension Framework (AXF) is automatically installed with Imaging. For information about configuring and using AXF and the AXF database tables, see *Oracle WebCenter Administrator's Guide for Application Adapters*.

For Oracle Application Extension Framework (AXF) to work with Imaging Managed Servers that run in a cluster or other distributed configuration, you need to configure the Java Object Cache (JOC) to be distributed to all of the Managed Servers.

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

6.5.1 Configuring the Java Object Cache for AXF in Distributed Imaging Managed Servers

For Oracle Application Extension Framework (AXF) in Imaging Managed Servers that run in a cluster, you need to configure a Java Object Cache (JOC) to be distributed to all of the Managed Servers. You can use HA Power Tools from the Oracle WebLogic Server Administration Console to configure the JOC for all of the Imaging Managed Servers that run in distributed mode.

> **Note:** After configuring the Java Object Cache, restart all affected Managed Servers for the configurations to take effect. For more information, see Section 9.3, "Restarting a Managed Server."

In the following instructions, *MW_HOME* represents the path to a Middleware home, where Oracle Fusion Middleware is installed, and *DomainHome* represents the path to the Oracle home for an Oracle WebLogic Server domain.

To configure the Java Object Cache for a cluster of distributed Managed Servers:

1. Enable HA Power Tools in the Oracle WebLogic Server Administration Console:

    a. Copy the following two WAR files from the *MW_HOME*/oracle_ common/hapowertools directory to the *DomainHome*/console-ext directory:

    * powertools-core.war

    * powertools-configurejoc.war

    For example:

    ```
    cd middlewarehome
    cp oracle_common/hapowertools/powertools-co* user_projects/domains/base_
    domain/console-ext/
    ```

    b. Restart the Oracle WebLogic Server Administration Server.

    For more information, see Section 9.1, "Starting the Administration Server," and Section 9.3, "Restarting a Managed Server."

    c. Access the Oracle WebLogic Server Administration Console (at http://*adminServerHost*:*adminServerPort*/console), and click the name of your domain in the left navigation tree.

    The **HA Power Tools** tab appears on the Settings page for the domain.

2. Configure the distributed cache:

   a. On the Settings page for your domain in the Administration Console, click the **HA Power Tools** tab.

   b. On the **Configure JOC** tab, select **Configure JOC for Clusters**.

   c. In the **Cluster Name** field, choose a cluster name from the list.

   d. In the **Discover Port** field, enter the listener port number for the cluster.

   e. In the **Hosts** field, enter the names of all the Managed Server hosts, separated by commas.

   f. Click the **Configure JOC** button.

3. Restart the cluster of Managed Servers.

4. Verify the JOC distributed cache mode:

   a. From the Middleware home on the host for one of the Managed Servers, run the CacheWatcher utility, as in the following example:

```
java -classpath oracle_common/modules/oracle.javacache_
11.1.1/cache.jar:oracle_common/modules/oracle.odl_11.1.1/ojdl.jar
oracle.ias.cache.CacheUtil watch -config=user_projects/domains/base_
domain/config/fmwconfig/servers/IPM_server2/javacache.xml
```

In this example, the class paths for the two JAR files are relative to the current directory (*MW_HOME*).

The `javacache.xml` file is the file used by one of the Imaging servers that is participating in the JOC distributed cache. For a distributed Java cache with either virtual or physical IP addresses, the listener address needs to be set in `javacache.xml`. Each of the files should contain all the distributor location entries but only one `<listener-address>` entry, set to the same port number for every cache member, as follows:

```
<listener-address port="portNumber1" host="hostName1"/>
<distributor-location ssl="true" port="portNumber1" host="hostName1"/>
<distributor-location ssl="true" port="portNumber1" host="hostName2"/>
<distributor-location ssl="true" port="portNumber1" host="hostName3"/>
<distributor-location ssl="true" port="portNumber1" host="hostName4"/>
```

   b. Enter the `lc` command to list the cache information:

```
INFO: JOC is initialized from oracle.ias.cache.CacheUtil.main, . . .
cache> lc
```

   c. In the output from the `lc` command, check that the Distributor Table shows an entry for each member of the distributed cache.

   d. Enter the `exit` command to stop the CacheWatcher utility.

For more information, see "Using HA Power Tools" and "Running CacheWatcher" in *Oracle Fusion Middleware High Availability Guide*.

6.5.2 Verifying the AXF Installation with HelloWorld

Follow these steps to enable the `HelloWorld` solution:

1. As user who owns the Imaging schema, run the `insertHelloCommand.sql` script from the following directory:

   - **UNIX path:**
     MW_HOME/*WC_CONTENT_ORACLE_HOME*/axf/drivers/HelloWorld/dbscripts

   - **Windows path:**
     MW_HOME*WC_CONTENT_ORACLE_HOME*\axf\drivers\HelloWorld\dbscripts

   ---

   Note: For IBM DB2 only, add the following line to beginning of the `insertHelloCommand.sql` script before you run it:

   `CONNECT TO soadb USER am3_ipm USING oracle;`

   ---

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

   `http://`*host*`:`*port*`/imaging/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.

6.5.3 Verifying the AXF Installation with HelloBpel

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 following directory:

- **UNIX path:**
  MW_HOME/*WC_CONTENT_ORACLE_HOME*/axf/drivers/HelloBpel

- **Windows path:**
  MW_HOME*WC_CONTENT_ORACLE_HOME*\axf\drivers\HelloBpel

To enable the HelloBpel solution:

1. Run one of the following `HelloBPEL` SQL scripts:

   ■ **UNIX scripts:**

      MW_HOME/WC_CONTENT_ORACLE_HOME/axf/drivers/HelloBpel/dbscripts
      /oracle/insertHelloBPELData.sql

      MW_HOME/WC_CONTENT_ORACLE_HOME/axf/drivers/HelloBpel/dbscripts
      /sqlserver-db2/insertHelloBPELData.sql

   ■ **Windows scripts:**

      MW_HOME\WC_CONTENT_ORACLE_HOME\axf\drivers\HelloBpel\dbscripts
      \oracle\insertHelloBPELData.sql

      MW_HOME\WC_CONTENT_ORACLE_HOME\axf\drivers\HelloBpel\dbscripts
      \sqlserver-db2\insertHelloBPELData.sql

   If your database is Oracle, then run the script from the `oracle` directory.

   If your database is IBM DB2 or Microsoft SQL Server, then run the script from the `sqlserver-db2` directory.

   For IBM DB2 only, before you run the `HelloBPEL` SQL script, make the following changes to it:

   ■ Add this line to beginning of the script:

      ```
      CONNECT TO soadb USER am3_ipm USING oracle;
      ```

   ■ Change the following line to specify whatever the actual BPEL Connection is in the Oracle IPM **Manage Connections** section:

      ```
      Insert into AXF_SOLUTION_ATTRIBUTES (SOLUTION_NAMESPACE,PARAMETER_
      KEY,PARAMETER_VALUE) values ('HelloBPEL','BPEL_CONNECTION','test');
      ```

2. Run the `insertHelloBPELData.sql` script.

3. With Oracle JDeveloper 11*g*, open `HelloBPEL.jws` from following directory:

   ■ **UNIX path:**
      MW_HOME/WC_CONTENT_ORACLE_HOME/axf/drivers/HelloBpel/bpel

   ■ **Windows path:**
      MW_HOME\WC_CONTENT_ORACLE_HOME\axf\drivers\HelloBpel\bpel

   Deploy the process to your BPEL server. For assistance with this task, consult the Oracle JDeveloper documentation.

   > **Note:** The HelloBPEL sample solution assigns instances to a group named `California` by default. You need to add the `California` group to the `myrealm` security realm through the Oracle WebLogic Server Administration Console.
   >
   > If you are using an alternate identity store, such as Oracle Internet Directory, you can change the group assignment by modifying the `HelloBpelHumanTask.task` file within Oracle JDeveloper before deployment.

4. Access the driver page of the AXF web application using the following URL:

   `http://host:port/imaging/faces/Driver.jspx`

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

   - Solution Namespace: `HelloBPEL`

   - Command Namespace: `StartHelloBPEL`

   - User Name: A valid Imaging user; for example, `weblogic`

   The preceding Imaging user needs to be part of a group named California. If this group does not exist, then create it, and add the user to the group.

6. Click **Execute Command**.

   A response should be displayed in the response screen.

7. 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, create a new instance of `HelloBPELProcess`, and refresh the Task List.

6.6 Installing and Configuring Oracle Document Capture and Oracle Distributed Document Capture

Oracle Document Capture provides high-volume production scanning from a central location, while Oracle Distributed Document Capture provides a user-friendly web interface that enables distributed enterprises to capture images easily from remote locations.

For information about installing and configuring Oracle Document Capture, see the *Oracle Document Capture Installation Guide* and *Oracle Document Capture Administrator's Guide*.

For information about installing and configuring Oracle Distributed Document Capture, see the *Oracle Distributed Document Capture Installation Guide* and *Oracle Distributed Document Capture Administrator's Guide*.

The Imaging 11*g* Commit Driver is required to commit documents from either capture application to WebCenter Content. For information about using the Imaging 11*g* Commit Driver, see the *Oracle Distributed Document Capture Installation Guide* or *Oracle Distributed Document Capture Administrator's Guide*.

7

Completing the Oracle IRM Configuration

This chapter explains how to complete the initial configuration of Oracle Information Rights Management (Oracle IRM) in an Oracle WebLogic Server domain.

This chapter includes the following sections:

- Section 7.1, "Completing the Initial Oracle IRM Configuration"
- Section 7.2, "Validating the Oracle IRM Configuration"
- Section 7.3, "Configuring the Identity Store"
- Section 7.4, "Integrating Rights with Oracle Access Manager 11g"
- Section 7.5, "Configuring Oracle IRM to Use Oracle RAC"

7.1 Completing the Initial Oracle IRM Configuration

Before logging in to the Oracle IRM Management Console or using Content application server 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

> **Note:** In a production environment, Oracle WebCenter Content 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. For more information, see Section 3.9, "Reassociating the Identity Store with an External LDAP Authentication Provider."

7.1.1 Setting the Server URL Configuration Parameter for Oracle IRM

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

> **Caution:** The Server URL value is embedded into every sealed document, and Rights Desktop uses this value to identify and connect to an Content application server Management Server (Rights 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 Rights Desktop, this value will be the URL of the Oracle IRM Managed Server. For example:

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

To set the Server URL configuration parameter:

1. Start 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.example.com: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 farm navigation tree on the left, expand **WebCenter Content** and **Rights**, 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 a simple installation where the Managed Server is directly accessible to Rights Desktop, this value will be the URL of the Oracle IRM Managed Server, ending in `irm_desktop`:

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

   The `managedServerHost` value is the name of the host where the Managed Server is running, such as `myhost.example.com`. The default SSL port for Oracle IRM (`managedServerPort` value) is `16101`.

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

5. Click **Apply**.

7.1.2 Configuring a Key Store for Oracle IRM

The Oracle IRM Java EE application uses a cryptographic key to wrap (encrypt) and unwrap (decrypt) Oracle IRM sealed content keys stored in the database. This wrapping key, `oracle.irm.wrap`, must be generated and stored in a key store before contexts can be created.

Access to the key store requires a password, and access to the wrapping key requires an additional password. Both passwords are stored in the credential store.

To configure a key store for Oracle IRM, you need to do the tasks described in these topics:

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

- Creating a Key Store

- Setting the Key Store Location

- Adding Key Store Passwords to the Credential Store

- Configuring the Policy and Credential Store

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

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. 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 because it is the stronger encryption algorithm. Other platforms require an RSA key wrapping algorithm.

7.1.2.1.1 AES Algorithm With the AES algorithm, the size of the wrapping key can be 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.

> **Note:** Before you can use AES with a 256-bit key size, the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files need to be installed in the JRE directory of Oracle WebLogic Server. For more information about downloading the policy files, see the Java SE Downloads page on the Oracle Sun Technology Network at
>
> http://www.oracle.com/technetwork/java/javase/downloads/index.html

7.1.2.1.2 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.

7.1.2.2 Creating a Key Store

The `keytool` command will generate a key store, which requires a password to open. Inside the key store, a key, `oracle.irm.wrap`, will be stored, and access to this key requires an additional password.

To create a key store for Oracle IRM:

1. Run the `setWLSEnv` script to set the environment:

   - **UNIX script:**
     MW_HOME/wlserver_10.3/server/bin/setWLSEnv.sh

   - **Windows script:**
     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 or *MW_HOME*\wlserver_10.3\server\lib directory.

Setting the environment correctly results in keytool being in the user's PATH environment variable. This setting specifies the directory path to use for the keytool command in the rest of this procedure.

2. Run the keytool utility to generate a Oracle IRM key store.

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

   ```
   keytool -genseckey -storetype JCEKS -alias oracle.irm.wrap
         -keyalg AES -keysize 128 -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, on a single command line:

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

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

3. Copy the irm.jceks or irm.jks file to the domain's fmwconfig directory:

   ■ **UNIX path:**
   MW_HOME/user_projects/domains/*DomainHome*/config/fmwconfig

   ■ **Windows path:**
   MW_HOME\user_projects\domains*DomainHome*\config\fmwconfig

7.1.2.3 Setting the Key Store Location

The Rights Server configuration needs to be updated so that it can locate the key store file. You can set the key store location in the server configuration with either Fusion Middleware Control, on the Oracle IRM General Settings page, or with the WebLogic Scripting Tool (WLST) connect and setIRMKeyStore commands.

Note: If SSL is enabled, before you use WLST to connect to the Administration Server, you must either append the following parameters to the JVM_ARGS section of the wlst.sh file or set them in the CONFIG_JVM_ARGS environment variable:

```
-Dweblogic.security.SSL.ignoreHostnameVerification=true
-Dweblogic.security.TrustKeyStore=KeyStoreName
```

KeyStoreName is the name of the keystore in use (DemoTrust for the built-in demonstration certificate). The wlst.sh file is in the bin subdirectory of the common directory in the WebCenter Content Oracle home directory.

The suggested location for the key store is in a directory under the domain home:

- **UNIX path:**
  MW_HOME/user_projects/domains/*DomainHome*/config/fmwconfig

- **Windows path:**
  MW_HOME\user_projects\domains*DomainHome*\config\fmwconfig

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 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.example.com: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 farm navigation tree on the left, expand **WebCenter Content** and **Rights**, and then click **IRM**.

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

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

   - JCEKS if you are using an AES key

   - JKS if you are using an RSA key-pair

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

   - Key store path for a JCEKS key store:

     - **UNIX path:** *MW_HOME*/user_projects/domains /*DomainHome*/config/fmwconfig/irm.jceks

     - **Windows path:** *MW_HOME*\user_projects\domains *DomainHome*\config\fmwconfig\irm.jceks

   - Key store path for a JKS key store:

     - **UNIX path:** *MW_HOME*/user_projects/domains /*DomainHome*/config/fmwconfig/irm.jks

     - **Windows path:** *MW_HOME*\user_projects\domains *DomainHome*\config\fmwconfig\irm.jks

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

7. Click **Apply**.

To set the key store location with WLST commands:

1. Enter the following WLST commands:

   – **UNIX operating system**

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

   – **Windows operating system**

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

   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:

   ```
   't3://myHost.example.com:7001'
   ```

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

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

   – JCEKS if you are using an AES key

   – JKS if you are using an RSA key-pair

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

   – Key store path for an AES key store

     UNIX path: *MW_HOME*/user_projects/domains
     /*DomainHome*/config/fmwconfig/irm.jceks

     Windows path: *MW_HOME*\user_projects\domains
     DomainHome\config\fmwconfig\irm.jceks

   – Key store path for an RSA key store

     UNIX path: *MW_HOME*/user_projects/domains/
     DomainHome/config/fmwconfig/irm.jks

     Windows path: *MW_HOME*\user_projects\domains
     DomainHome\config\fmwconfig\irm.jks

7.1.2.4 Adding Key Store Passwords to the Credential Store

You must add passwords for the Oracle IRM key store to the credential store with
WLST commands. A key store password and a password for the generated key were
set when the key store was created. These passwords are required by the Rights.

To add key store passwords to the credential store:

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

  – **UNIX operating system**

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

– **Windows operating system**

```
WC_CONTENT_ORACLE_HOME\oracle_common\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")
```

Notes:

■ 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 key store.

■ 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.

■ For an RSA key store, enter the following WLST commands:

– **UNIX operating system**

```
WC_CONTENT_ORACLE_HOME/oracle_common/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")
```

– **Windows operating system**

```
WC_CONTENT_ORACLE_HOME\oracle_common\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")
```

Notes:

■ 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 key store.

■ 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.

7.1.2.5 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 3.9, "Reassociating the Identity Store with an External LDAP Authentication Provider."

7.2 Validating the Oracle IRM Configuration

When the Oracle IRM Managed Server is running, the Oracle IRM application is deployed to the Oracle WebLogic Server domain. You can validate that the configuration of the Managed Server was successful by accessing this URL:

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

For example:

```
https://myhost.example.com:16101/irm_desktop
```

7.3 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 3.9, "Reassociating the Identity Store with an External LDAP Authentication Provider."

7.4 Integrating Rights with Oracle Access Manager 11g

Oracle Access Manager is the recommended single sign-on (SSO) solution for Oracle WebCenter Content applications. It provides flexible and extensible authentication and authorization, as well as audit services. You can integrate Oracle IRM with Oracle Access Manager by configuring both of them for the integration.

Oracle IRM supports Basic authentication with Oracle Access Manager, which contains an authorization engine that 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.

Oracle IRM currently has limited support for SSO through Oracle Access Manager 11g, as described in this section.

Public URIs need to be specified for Oracle Access Manager 11g:

- `/irm_rights`

- `/irm_rights/.../*`

Rights Desktop does not support Oracle Access Manager 11g.

You also need to protect the following URI:

- `/irm_rights/faces`

Implementation of single sign-on (SSO) with the Oracle IRM 11g server management console will enable access to applications as expected. Input of a valid user name and password combination during the same SSO session will be recognized.

Implementation of SSO for Rights Desktop with Oracle Access Manager 10g is possible but will not enable access to multiple applications in the same session by entry of a single username and password combination. Rights Desktop users will be prompted

for a user name and password even if they have already supplied a valid user name and password within the same SSO session. This level of support for SSO is provided so that users can be shown a recognizable sign-on dialog that will indicate the correct user name and password combination to be entered.

> **Notes:**
>
> - Rights Desktop is supported only with Oracle Access Manager 10*g* and not with Oracle Access Manager 11*g* for Release 11.1.1.6.0.
>
> - For information about Oracle Access Manager 10*g*, see the *Oracle Access Manager Access Administration Guide*.
>
> - For information about configuring Windows Native Authentication (WNA), see "Configuring Single Sign-On with Microsoft Clients" in *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

After you install and configure Oracle Access Manager 11*g*, you can configure it and Oracle IRM to work together.

> **Note:** The following procedure should be performed only after you have installed Oracle WebCenter Content (described in Chapter 2, "Installing Oracle WebCenter Content") and configured a Oracle IRM Managed Server (described in Chapter 3, "Configuring Oracle WebCenter Content Applications"). You should also have configured and tested any required connections.

To configure Oracle IRM and Oracle Access Manager 11g to work together:

1. Install Oracle Access Manager 11*g*, as described in "Installing the Oracle Identity Management 11g Software" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

2. Configure Oracle Access Manager 11*g*, as described in "Configuring Oracle Access Manager" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

3. Install and configure Oracle HTTP Server (OHS), as described in "Installing Oracle Web Tier" in the *Oracle Fusion Middleware Installation Guide for Oracle Web Tier*.

4. Install and configure WebGate, as described in "Installing and Configuring Oracle HTTP Server 11g Webgate for OAM" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

5. Append Oracle WebCenter Content URIs to forward to the `mod_wl_ohs.conf` file, as in the following example:

```
# IRM management web site
<Location /irm_rights>
      SetHandler weblogic-handler
      WebLogicHost managedServerHost
      WebLogicPort managedServerPort
</Location>
```

In the preceding example, `managedServerHost` represents the host name of the machine hosting Oracle IRM, and `managedServerPort` represents the port number of the Oracle WebLogic Server instance hosting Oracle IRM.

> **Note:** The entries in the preceding `Location` element are used by the web server to forward requests that match the URL pattern (for example, `/irm_rights`) to the Oracle IRM Managed Server.

The `Location` element in the next example specifies a host and port number:

```
<Location /irm_rights>
  SetHandler weblogic-handler
  WebLogicHost irm.example.com
  WebLogicPort 16100
</Location>
```

6. Log in to the Oracle Access Manager console, as described in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*, and follow the instructions in the administrator's guide to do these tasks:

   a. Create a new Application Domain called `IRM Domain`.

   b. Select **IRM Domain**, then **Resources**, and then create entries for all the Oracle IRM URLs:

      * `/irm_rights`

      * `/irm_rights/.../*`

      * `/irm_rights/faces`

      * `/irm_rights/faces/.../*`

   c. Select **IRM Domain**, then **Authentication Policies**, and then create a Protected Policy and a Public Policy.

   d. In the Authentication Protected Policy, add these Oracle IRM resources:

      * `/irm_rights/faces`

      * `/irm_rights/faces/.../*`

   e. In the Authentication Public Policy, add these Oracle IRM resources:

      * `/irm_rights`

      * `/irm_rights/.../*`

   f. Select **IRM Domain**, then **Authorization Policies**, and then create a Protected Policy and a Public Policy.

   g. Add the same Oracle IRM protected and public resources to the Protected Policy and the Public Policy, to match the Authentication policies.

7. Configure the Oracle WebCenter Content domain by performing these tasks:

   a. Add and configure the Oracle Access Manager ID Asserter.

   b. Add and configure Oracle Internet Directory.

   c. Add the OPSS (Oracle Access Manager) SSO provider.

   For more information about these tasks, see "Deploying the Oracle Access Manager 11g SSO Solution" in the *Oracle Fusion Middleware Application Security Guide*.

8. Test the Oracle Access Manager installation.

   After installing and configuring Oracle Access Manager 11*g*, check that you can access all of the configured applications and that the global login and logout is giving you access to all of your configured applications without prompting you to sign in again. Also test global logout, where available, and make sure you are logged out of all other related applications.

   For example, if `mod_wl_ohs.conf` redirects `/irm_rights` to `irm.example.com:16100` and if OHS is listening on the port `oam.example.com:7778`, then the IRM Rights application can be accessed through `https://oam.example.com:7778/irm_rights`, provided Oracle Access Manager has been set up correctly. After authentication, Oracle Access Manager will internally delegate requests to `https://irm.example:16100/irm_rights`.

7.5 Configuring Oracle IRM to Use Oracle RAC

To use Oracle RAC with an Oracle IRM instance, the Oracle IRM data source needs to be altered using the Oracle WebLogic Server Administration Console and the following procedure:

1. From **Services**, select **JDBC**, and then select **DataSources**

2. Select the Oracle IRM data source.

3. On the **Transaction** tab, check **Supports Global Transactions**, then check **Emulate Two-Phase Commit**.

4. Click **Save**.

This will set the `global-transactions-protocol` for Oracle IRM data sources for Oracle RAC to `EmulateTwoPhaseCommit`.

8

Completing the Records Configuration

This chapter explains how to complete the initial configuration of Oracle WebCenter Content: Records in an Oracle WebLogic Server domain.

This chapter includes the following sections:

- Section 8.1, "Completing the Initial Records Configuration"
- Section 8.2, "Using OracleTextSearch with Records"
- Section 8.3, "Setting Connection Pool Property Values for an IBM DB2 Data Source"
- Section 8.4, "Installing and Configuring Desktop on a Client Workstation"

8.1 Completing the Initial Records Configuration

After installation and startup, when you go to the web interface for Records, you will get the WebCenter Content: Records Configuration page, which Figure 8–1 shows.

Figure 8–1   Configuration Page for Records

WebCenter Content: Records Configuration

Node Information

Cluster Node Identifier:	ⓘ	URM_server1
* Content Server Instance Folder:	ⓘ	/middlewarehome/user_projects/domains/test
* Native File Repository Location:	ⓘ	/middlewarehome/user_projects/domains/test
* Weblayout Folder:	ⓘ	/middlewarehome/user_projects/domains/test
* User Profile Folder:	ⓘ	/middlewarehome/user_projects/domains/test
Content Server URL Prefix:	ⓘ	/urm/

Instance Information

Is New Content Server Instance:	ⓘ	☑
Server Socket Port:	ⓘ	
Incoming Socket Connection Address Security Filter:	ⓘ	127.0.0.1|0:0:0:0:0:0:0:1
* Web Server HTTP/HTTPS Address:	ⓘ	myhost.example.com:16300
Web Address Is HTTPS:	ⓘ	☐
Company Mail Server:	ⓘ	mail
Administrator E-Mail Address:	ⓘ	sysadmin@example.com
* Server Instance Name:	ⓘ	myhostexamplecom16300
* Server Instance Label:	ⓘ	myhostexamplecom16300
* Server Instance Description:	ⓘ	Instance myhostexamplecom16300
Is Auto Number Enabled:	ⓘ	☑
Auto Number Prefix:	ⓘ	middlewareexam

Search Information

FullText Search Option:	ⓘ	None ▾
External DataSource:	ⓘ	

* - Required

Submit   Reset

For information about the fields on this page and the values you can enter to configure your Records instance, see Section 4.3.2, "Configuring the Content Server Instance." After you complete the WebCenter Content: Records Configuration page and clicking the **Submit** button, you need to restart Records, as described in Section 9.3, "Restarting a Managed Server."

When Records restarts, the web interface shows an alert, "Initial Records Management Setup is Not Complete!" Then you can select the Records install settings and installation level you want on the Configure: Enabled Features page and configure the features. For information about configuring these settings, see Section 8.1.1, "Configuring the Level of Records Features."

After you configure the installation level and features, you can complete the Records configuration through the Setup Checklist page. For more information, see Section 8.1.2, "Completing the Setup Checklist for Records."

> **Note:**   The ContentFolios component is required for access to the Records web interface. This component is enabled by default in a Records Managed Server. Do not disable the ContentFolios component.

8.1.1 Configuring the Level of Records Features

On the Enabled Features page, you can configure and installation level and features for Records. The default installation level is **Minimal**.

To configure the level of Records features:

1. From the **Records** menu, choose **Configure**, then choose **Enabled Features**, as Figure 8–2 shows.

Figure 8–2   Records Menu
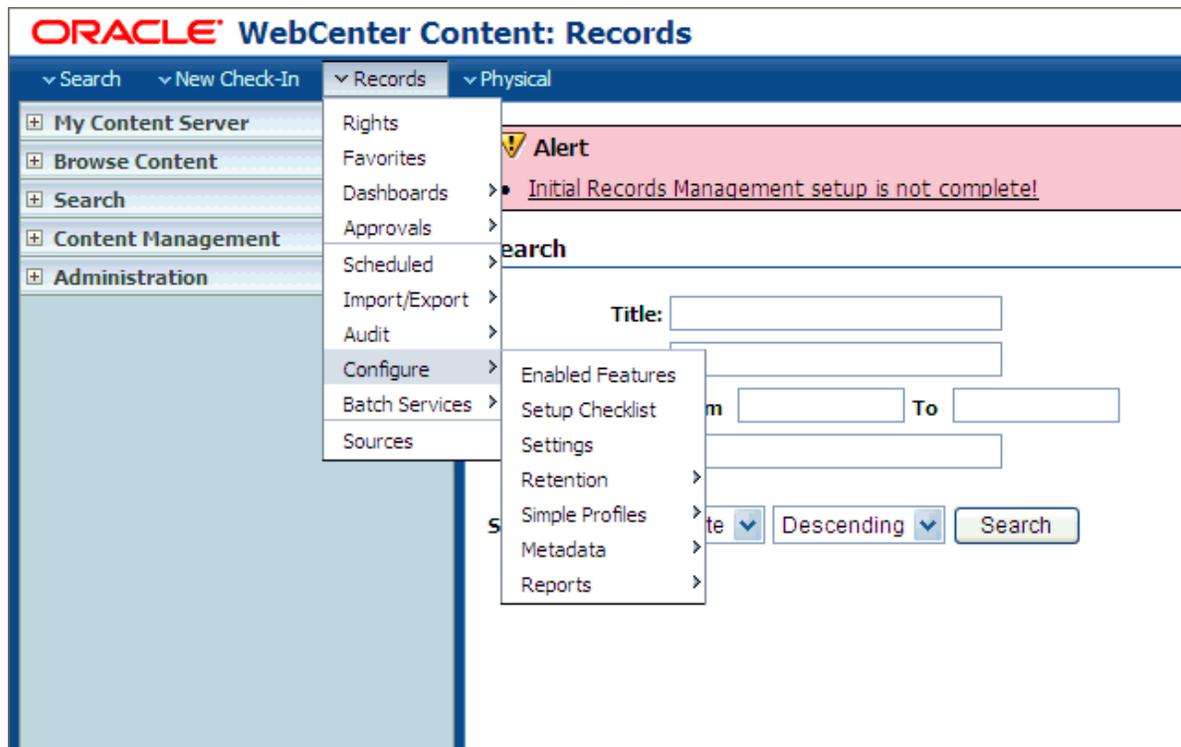
2. On the Enabled Features page, which Figure 8–3 shows, select an installation level, which selects all the features and disposition actions for that level.

Figure 8–3   Enabled Features Page

The following table describes the installation levels and features that can be enabled. For information about the components to be enabled for each level, and the features and disposition actions to be installed, click the **Info** icon next to the level.

Element	Description
Installation Level	Specifies the type of configuration to be enabled: ■ Minimal ■ Typical ■ DoD Baseline ■ DoD Classified ■ Custom

Element	Description
Features	When you select an installation level, the default features for that level are selected to be enabled. If you select the **Custom** installation level, you can select the features you want enabled: ■ Related Content ■ Audit Trigger ■ Subject to Review ■ Revision Dates ■ Security Markings ■ Email Fields ■ DoD Configuration ■ Classified Topics ■ FOIA/Privacy Act
Disposition Actions	This section contains the disposition actions that can be used for content: ■ Activate ■ Rescind ■ Approve Deletion ■ Obsolete ■ Expire ■ Destroy ■ Cancel ■ Cutoff

> **Note:** If you are using Oracle WebCenter with Records and want to use the DOD feature, you can set the DoD Baseline or Classified Installation level after WebCenterConfigure has been enabled and has had a chance to check in its conversion templates.
>
> If you select a DOD installation level first, you can create a rule that matches the documents created by WebCenterConfigure to assign them to a default category. The category could be based on the content IDs. For more information, see "Setting Up Workflows" in the *Oracle WebCenter Content Setup Guide for Records*.

3. If you selected the **Custom** installation level, select the features and disposition actions that you want enabled, and deselect any that you do not want enabled.

4. Click the **Submit** button.

After making selections or if configuration options are changed (for example, switching from **Baseline** to **Classified**), you need to restart the Records Managed Server and rebuild the Content Server index. For more information, see Section 8.1.2, "Completing the Setup Checklist for Records." For information about rebuilding the index, see "Working with the Search Index" in the *Oracle WebCenter Content System Administrator's Guide for Content Server*.

8.1.2 Completing the Setup Checklist for Records

After the installation and configuration of Records on a Managed Server, you need to complete the Setup Checklist page before you can set up retention policies and procedures. This page is used to set global options for aspects of the retention management system.

For information about setting up retention policies and procedures, see "Retention Options" in *Oracle WebCenter Content Setup Guide for Records*.

To complete the Setup Checklist for Records:

1. From the **Records** menu, choose **Configure** then choose **Setup Checklist**.

2. On the Setup Checklist page, which Figure 8–4 shows, for each action that is marked **Not Done**, click the action, complete the configuration for it, refresh the Setup Checklist page, and then mark the checkbox to the right of the action to indicate that it is complete.

Figure 8–4   Records Setup Checklist

If any required configuration tasks on this page are not completed, a warning message with a link to this page appears on the home page of the Records system. You can click the link to display this page, or you can display the page from the **Records** menu again.

> **Note:** The Configure Report Library task is only for the Records Management feature in Content Server. This library is not needed for Oracle WebCenter Content: Records. For information about how to configure the report library, see Section 4.1, "Configuring the Report Library for Records Management in Content Server."

3. For any of the other actions that you want to configure, click the action, complete the configuration for it, refresh the Setup Checklist page, and then mark the checkbox to the right of the action to indicate that it is complete.

Expanding any action in this list displays a detailed explanation of the action's purpose. The options available on the page depend on your installation level:

- **Minimal**
- **Typical**
- **DoD Baseline**
- **DoD Classified**
- **Custom**

The following table lists the actions that can be on the Setup Checklist and describes the purpose of each action.

Action	Description
Configure Installation	Used to configure optional components and metadata fields. Select from preset configurations to choose the features that are needed.
Configure Report Library	Used to configure the report library for the Records Management feature of Content Server, after adding the `oracle.xdo.runtime` library from the Oracle WebLogic Server Administration Console and a library reference to `weblogic-application.xml` This library is not needed for Oracle WebCenter Content: Records.
Define Defaults	Used to define the default for audit trails, template locations, and metadata for content that is automatically checked in on a periodic basis. You can configure metadata for Audit Entries and for Screening reports.
	Clicking an option brings up a check in page where you can edit the fields to be used as defaults.
Configure Security Settings	Used to define the security settings including roles, rights, and access control list use. This link opens the Admin Applets. Click the User Applet to configure security.
Configure Retention Management Settings	Used to configure many of the retention management options such as supplemental markings, triggers, and reports. Clicking this option displays the Configure Retention Settings page.
	For information about this page, see "Configure Retention Settings Page" in *Oracle WebCenter Content Setup Guide for Records*.

Action	Description
Configure Fiscal, Calendar, and Custom Periods	Used to set periods used for disposition processing. Selecting this option displays the Configure Periods page.
	For information about this page, see "Configure Periods Page" in *Oracle WebCenter Content Setup Guide for Records*.
Configure Global, Direct, and Indirect Triggers	Used to set up the triggers used for disposition processing. Selecting this option displays the Configure Triggers page.
	For information about this page, see "Configure Triggers Page" in *Oracle WebCenter Content Setup Guide for Records*.
Create Retention Schedule or Import Retention Schedule	Used to set up retention schedules. Selecting **Create Retention Schedule** displays the Exploring Retention Schedule page. Selecting Import Retention Schedule displays the Import/Export Screen.
	For information about importing and exporting files, see "Managing Imports and Exports" in *Oracle WebCenter Content Administrator's Guide for Records*.
Configure Freeze Reasons	Used to set up freezes. Selecting this option displays the Freeze Configuration page.
	For information about this page, see "Freeze Configuration Page" in *Oracle WebCenter Content Setup Guide for Records*.
Configure Workflows	Used to set up workflows to use with off-site storage, reservations, and category disposition processing. These workflows must be set up for that functionality to work properly.
	For more information, see "Setting Up Workflows" in *Oracle WebCenter Content Setup Guide for Records*.
Configure Default Reviewers	Used to add users who will be default reviewers. Click User Admin Applet to proceed.
Configure Related Content Types	Used to set up links. Selecting this option displays the Configure Links Type Page.
	For more information, see "Configuring Related Content (Links)" in *Oracle WebCenter Content User's Guide for Records*.
Configure Federated Search Default Category	Used to indicate a default category and default folder to use for Federated searches. Selecting this option displays the Admin Server page, where you can enter configuration variables:
	■ `FederatedSearchDefaultCategory=categoryId`
	■ `FederatedSearchDefaultFolder=folderId`
Configure 'Profile Trigger' as Trigger Field	Used to determine the trigger for profiles used in searching and checking in content and physical items.

There is no longer an installation requirement that the `NumConnections` configuration variable be set to 10. This configuration is now controlled by Oracle WebLogic Server and does not need to be set independently.

8.2 Using OracleTextSearch with Records

When you use `OracleTextSearch` with Content Server, 32 optimized fields are allowed. When Records is installed, the number of optimized fields can exceed the 32-field limit.

To accommodate this limitation, if `OracleTextSearch` is configured as the search engine, Records sets its date fields to be nonsearchable. Because of this, Records date fields will not appear on search pages.

If you install Records while using `OracleTextSearch` and later change search engines, you can configure the date fields to be searchable by using the Content Server Configuration Manager.

If you install Records without `OracleTextSearch` and later change your current search engine to `OracleTextSearch`, you must manually configure the date fields to be nonsearchable in the Content Server Configuration Manager.

To search auxiliary metadata in Records with Oracle Text 11*g*, you must configure Content Server to use `OracleTextSearch` as the search engine. You can set `OracleTextSearch` on the WebCenter Content postinstallation configuration page or in the configuration file. For more information, see Section 4.4, "Configuring OracleTextSearch for Content Server."

8.3 Setting Connection Pool Property Values for an IBM DB2 Data Source

If the Records Managed Server has an IBM DB2 data source, you need to set the `DynamicSections` property value to at least `500` in the connection pool configuration for the data source. This setting can prevent a `DYNAMICSECTIONS` error.

To set connection pool property values for an IBM DB2 data source:

1. 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.example.com: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.

2. Click **Services** in the navigation tree on the left.

3. Click **JDBC** in the **Section** column under Summary of Services.

4. Click **Data Source** in the **Section** column under Summary of Services: JDBC.

5. Click **URDMS**, or the JNDI name of the data source for the Records Managed Server, in the Data Sources table.

6. On the Settings page for the data source, click the **Connection Pool** tab.

7. In the **Properties** field, add the following lines to the list of properties to be passed to the JDBC driver:

   ```
   createDefaultPackage=true
   replacePackage=true
   dynamicSections=500
   ```

8. Click the **Save** button.

8.4 Installing and Configuring Desktop on a Client Workstation

The Oracle WebCenter Content: Desktop component provides a set of embedded applications that help you seamlessly integrate your desktop experience with Content Server. More specifically, it provides convenient access to Content Server from Microsoft Windows Explorer, desktop applications like Microsoft Word and Excel, and email clients like Microsoft Outlook and Lotus Notes.

For information about how to instal Desktop on a client workstation, see "Setting Up the Desktop Client Software on Your Computer" in *Oracle WebCenter Content User's Guide for Desktop*.

9

Verifying the Oracle WebCenter Content Configuration

This chapter explains how to verify the configuration of Oracle WebCenter Content and its applications.

This chapter includes the following sections:

- Section 9.1, "Starting the Administration Server"
- Section 9.2, "Starting Managed Servers"
- Section 9.3, "Restarting a Managed Server"
- Section 9.4, "Using Node Manager with Oracle WebCenter Content"
- Section 9.5, "Increasing the Java Heap Size for a Managed Server"
- Section 9.6, "Verifying the Configuration of Oracle WebCenter Content"

9.1 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.

> **Note:** On a Windows operating system that has User Account Control (UAC) enabled, you need to start the Administration Server and the WebCenter Content Managed Server as an administrator before you can access Content Server through the web interface for WebCenter Content.
>
> Open a Command Prompt window with the `Run As Administrator` option (right-click **Command Prompt** on the **Start** menu, or right-click the `C:\windows\system32\cmd.exe file`, and choose **Run As Administrator**). You should see "Administrator" in the title bar of the Command Prompt window.
>
> Then you can use this window to start the Administration Server, as described in the following procedure.

To start the Administration Server:

1. Run the `startWebLogic` script (from the `bin` directory under the domain home directory):

   - **UNIX script:** *MW_HOME*/user_projects/domains/*DomainHome*/bin /startWebLogic.sh [http://*admin_url*]

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

   - **Windows script:** *MW_HOME*\user_projects\domains*DomainHome* \bin\startWebLogic.cmd [http://admin_url]

   The directory path to the Middleware home (*MW_HOME*) and the name of the domain (*DomainHome*) were provided on the Specify Domain Name and Location screen in Fusion Middleware Configuration Wizard.

   The value of *admin_url* is the Administration Server URL. If the Administration Server does not use the default port, 7001, you need to specify a value for *admin_url*, such as http://localhost:8001/.

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.example.com: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.

9.2 Starting Managed Servers

You can start each Managed Server in your Oracle WebLogic Server domain from the `bin` directory under your domain home directory:

- **UNIX path:** *MW_HOME*/user_projects/domains/*DomainHome*/bin

- **Windows path:** *MW_HOME*\user_projects\domains*DomainHome*\bin

The directory path to the Middleware home (*MW_HOME*) and the name of the domain (*DomainHome*) were provided on the Specify Domain Name and Location screen in Fusion Middleware Configuration Wizard.

> **Important:**
>
> - Before starting an Imaging Managed Server and logging in for the first time, see Section 6.1, "Completing the Initial Imaging Configuration," and do not start the Managed Server until you have completed the tasks before Section 6.1.2, "Starting the Imaging Managed Server and Accessing the Web Client."
>
> - Before logging in to the Oracle IRM Management Console for the first time or using Content application server Desktop, see Section 7.1, "Completing the Initial Oracle IRM Configuration."
>
> - On a Windows operating system that has User Account Control (UAC) enabled, you need to start the Oracle WebLogic Server Administration Server and WebCenter Content Managed Server as an administrator before you can access Content Server through the web interface for WebCenter Content.
>
>   Open a Command Prompt window with the `Run As Administrator` option (right-click **Command Prompt** on the **Start** menu, or right-click the `C:\windows\system32\cmd.exe` file, and choose **Run As Administrator**). You should see "Administrator" in the title bar of the Command Prompt window.
>
>   Then you can use this window to start the WebCenter Content Managed Server, as described in the following procedure. For information about accessing Content Server, see Section 9.6, "Verifying the Configuration of Oracle WebCenter Content."

To start a Managed Server:

1. Start the Administration Server (see Section 9.1, "Starting the Administration Server").

2. Run the `startManagedWebLogic` script:

   - **UNIX script**: *MW_HOME*/user_projects/domains/*DomainHome*/bin/startManagedWebLogic.sh *server_name* [*admin_url*]

   - **Windows script**: *MW_HOME*\user_projects\domains*DomainHome*\bin\startManagedWebLogic.cmd *server_name* [*admin_url*]

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

   - `UCM_server1` (WebCenter Content)

   - `IBR_server1` (Inbound Refinery)

   - `IPM_server1` (Imaging)

   - `IRM_server1` (Oracle IRM)

   - `URM_server1` (Records)

   The Managed Servers names 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

The value of `admin_url` is the Administration Server URL. If the Administration Server does not use the default port, 7001, you need to specify a value for `admin_url`, such as `http://localhost:8001/`.

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.

For example, the following script would start an Imaging Managed Server on a UNIX operating system:

```
cd MW_HOME/user_projects/domains/domain_name/bin
./startManagedWebLogic.sh IPM_server1 http://localhost:8001/
```

On a Windows operating system, the following script would start a Oracle IRM Managed Server on the local host:

```
MW_HOME\user_projects\domains\domain_name\bin\
startManagedWebLogic.cmd IRM_server1
```

To avoid prompts for a user name and password on startup 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 file would include the following lines:

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

The `boot.properties` file will be encrypted the first time that the Managed Server is started.

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

9.3 Restarting a Managed Server

Before changes to the configuration of a Managed Server can take effect, you need to restart it. You can restart a Managed Server with the Administration Console, shutdown and startup scripts, or Fusion Middleware Control.

The following example shows how to restart a Managed Server with the `stopManagedWebLogic` and `startManagedWebLogic` scripts. For more information, see "Restarting Content Server" in *Oracle WebCenter Content System Administrator's Guide for Content Server*.

To restart a Managed Server with scripts on the command line:

1. Stop the Managed Server with the `stopManagedWebLogic` script.

   - **UNIX script:**
     `DomainHome`/bin/stopManagedWebLogic.sh UCM_server1

   - **Windows script:**
     `DomainHome`\bin\stopManagedWebLogic.cmd UCM_server1

2. Stop the Administration Server with the `stopWebLogic` script.

   - **UNIX script:** `DomainHome`/bin/stopWebLogic.sh

   - **Windows script:** `DomainHome`\bin\stopWebLogic.cmd

3. Start the Administration Server with the `startWebLogic` script.

- **UNIX script:** *DomainHome*/bin/startWebLogic.sh

- **Windows script:** *DomainHome*\bin\startWebLogic.cmd

4. Start the Managed Server with the `startManagedWebLogic` script.

- **UNIX script:**
  DomainHome/bin/startManagedWebLogic.sh UCM_server1

- **Windows script:**
  DomainHome\bin\startManagedWebLogic.cmd UCM_server1

9.4 Using Node Manager with Oracle WebCenter Content

The Oracle WebLogic Server Node Manager enables you to start and stop Oracle WebLogic Server instances remotely, monitor them, and automatically restart them after an unexpected failure. You can configure Oracle WebCenter Content Managed Servers, the Administration Server, and Node Manager to work together in an Oracle WebLogic Server domain. Node Manager is installed on all the machines that host any server instance.

Before you can use Node Manager to start and stop Oracle WebCenter Content Managed Servers in a domain, you need to do these configuration tasks:

- Configure at least one machine for the domain.

- Assign the Administration Server and Managed Servers (such as `AdminServer`, `IPM_server1`, and `UCM_server1`) to one or more machines.

- Enable Node Manager to use the Oracle WebCenter Content startup scripts by setting the `StartScriptEnabled` property in the `nodemanager.properties` file to `true`.

This section describes how to configure a machine in an Oracle WebLogic Server domain, assign the Administration Server and Managed Servers to a machine, and enable Node Manager to use startup scripts before you start it. For information about creating or extending a domain to configure Oracle WebCenter Content, see Chapter 3, "Configuring Oracle WebCenter Content Applications."

9.4.1 Configuring a Machine

The Administration Server uses a machine definition and the Node Manager application to start remote servers. During the initial configuration of Oracle WebCenter Content, you can configure machines through the Fusion Middleware Configuration Wizard. After the initial configuration, you can configure machines through the Oracle WebLogic Server Administration Console.

To configure a machine through the Fusion Middleware Configuration Wizard:

1. When you get to the Select Optional Configuration screen in the Fusion Middleware Configuration Wizard, be sure to select **Managed Servers, Clusters and Machines**.

2. On the Configure Machines screen, click **Add**.

3. Specify values for these fields:

- **Name**

  Enter a valid machine name, such as **Linux-Box**. The machine name identifies the machine within the Oracle WebLogic Server domain; it does not have to match the network name for the machine. The name must be unique within the domain.

- **Node manager listen address**

  Select a value from the drop-down list for the listen address used by Node Manager to listen for connection requests. By default, the IP addresses defined for the local system and `localhost` are shown in the drop-down list. The default value is `localhost`.

  If you specify an IP address for a machine that hosts the Administration Server and you need to access Node Manager, you must disable host name verification. For more information, see "Using Host Name Verification" in *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

- **Node manager listen port**

  Enter a valid value for the listen port used by Node Manager to listen for connection requests. The valid listen port range for Node Manager is from `1` to `65535`. The default value is `5556`.

9.4.2 Assigning Servers to a Machine

During the initial configuration of Oracle WebCenter Content, you can assign the Administration Server and Managed Servers to one or more machines through the Fusion Middleware Configuration Wizard.

After the initial configuration, you can assign Managed Servers to machines through the Oracle WebLogic Server Administration Console.

To assign servers to a machine through the Fusion Middleware Configuration Wizard:

1. On the Assign Servers to Machines screen, select one or more servers in the Server area

2. Click the right arrow button to assign the selected server or servers to a machine.

3. Click **Next** when you are done.

9.4.3 Enabling the Use of Startup Scripts Before Starting Node Manager

Before you start Node Manager the first time, you can run the `setNMProps.sh` script to set the `StartScriptEnabled` property to `true`. This setting is required for Node Manager to start the Managed Servers with startup scripts. You must use the `StartScriptEnabled` property to avoid class-loading failures and other problems.

If you enable Node Manager to use startup scripts on a machine that hosts one or more Managed Servers that are assigned to a machine, you can 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.

For a Records Managed Server, before you start Node Manager, be sure to complete the Records setup checklist, described in Section 8.1, "Completing the Initial Records Configuration."

To enable startup scripts and start Node Manager:

1. Navigate to the following directory

   MIDDLEWARE_HOME/oracle_common/common/bin
   MIDDLEWARE_HOME is the directory where Oracle Fusion Middleware is installed.

2. Run the `setNMProps.sh` script to set the `StartScriptEnabled` property to `true` before starting Node Manager:

   ./setNMProps.sh

   This is a one-time action. After you run this script, you can skip this step before starting Node Manager again.

3. Start Node Manager with the `startNodeManager` script.

   UNIX script: *WL_HOME*/server/bin/startNodeManager.sh

   Windows script: *WL_HOME*\server\bin\startNodeManager.cmd

   WL_HOME is the directory where Oracle WebLogic Server is installed.

   > **Note:** On a Windows operating system that has User Account Control (UAC) enabled, you need to start the Oracle WebLogic Server Administration Server and the WebCenter Content Managed Server as an administrator before you can access Content Server through the web interface for WebCenter Content. If you want to use Node Manager to start the WebCenter Content Managed Server, you also need to start Node Manager as an administrator, with the following procedure:
   >
   > 1. Run *DomainHome*\ucm\cs\bin\Installer.exe DisableNtfs8dot3 to disable the 8-dot-3 naming convention on the Windows operating system.
   >
   >   On a Windows 7 operating system, instead of running this script, you need to change the Registry key directly, as described in Section 2.1.1, "Disabling the 8.3 File Naming Convention on a Windows Operating System."
   >
   > 2. Restart the machine.
   >
   > 3. Open a Command Prompt window with the `Run As Administrator` option (right-click **Command Prompt** on the **Start** menu, or right-click the `C:\windows\system32\cmd.exe` file, and choose **Run As Administrator**). You should see "Administrator" in the title bar of the Command Prompt window.
   >
   > 4. Start the Oracle WebLogic Server Administration Server.
   >
   >   For more information, see Section 9.1, "Starting the Administration Server."
   >
   > 5. Open another Command Prompt window with the `Run As Administrator` option.
   >
   > 6. Start Node Manager, as described in Section 9.4.3, "Enabling the Use of Startup Scripts Before Starting Node Manager."
   >
   > 7. Access the Oracle WebLogic Server Administration Console, click **Servers**, and start the WebCenter Content Managed Server.
   >
   >   For information about accessing the Administration Console, see Section 9.6, "Verifying the Configuration of Oracle WebCenter Content."

For more information about Node Manager, see *Managing Server Startup and Shutdown for Oracle WebLogic Server* and *Node Manager Administrator's Guide for Oracle WebLogic Server*.

9.5 Increasing the Java Heap Size for a Managed Server

The default Java heap size is 512 MB for an Oracle WebLogic Server Managed Server. For better performance with the JRockit JDK, increase the heap size for each Managed Server in an Oracle WebCenter Content domain to 1 GB (1024 MB). If you use Node Manager to start the Managed Servers, you can specify a heap size as a Java argument on the **Server Start** tab of the Settings page for each Managed Server in the Administration Console.

To increase the Java heap size for a Managed Server in the Administration Console:

1. Log into the Administration Console.

2. If you have not already done so, in the Change Center on the upper left, click **Lock & Edit**.

3. In the navigation tree on the left, expand **Environment**, and click **Servers**.

4. In the **Servers** table, click the name of the server instance you want to configure.

5. On the **Configuration** tab, click **Server Start**.

6. In the **Arguments** field, specify the following Java option:

   ```
   -Xmx1024m
   ```

7. Click **Save**.

8. To activate the change, in the Change Center on the upper left, click **Activate Changes**.

9. Restart the Managed Server, as described in Section 9.3, "Restarting a Managed Server."

9.6 Verifying the Configuration of Oracle WebCenter Content

To verify the configuration of Oracle WebCenter Content, start a web browser, and enter the following URLs to test access to the 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.example.com: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.example.com: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.example.com: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 WebCenter Content applications.

- To test WebCenter Content by accessing Content Server:

  `http://managedServerHost:managedServerPort/cs`

  The default port number for WebCenter Content is `16200`.

  The first user to log in to Oracle WebCenter Content Server must be the administrator of the Oracle WebLogic Server domain, to complete the configuration of Content Server. For more information, see Section 4.2, "Completing the Initial WebCenter Content Configuration," and "Introduction to Content Server Administration," "Managing Security and User Access," and "Starting, Stopping, and Restarting Content Server" in *Oracle WebCenter Content System Administrator's Guide for Content Server*.

- To test a newly set up Inbound Refinery instance:

  `http://managedServerHost:managedServerPort/ibr`

  Log in with the user name and password for Oracle WebLogic Server. The default port number for Inbound Refinery is `16250`.

- To test a newly set up Imaging instance:

  `http://managedServerHost:managedServerPort/imaging`

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

- To test a newly set up Oracle IRM instance:

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

- To test a newly set up Records instance:

  `http://`*`managedServerHost`*`:`*`managedServerPort`*`/urm`

  Log in with the user name and password for Oracle WebLogic Server. The default port number for Records is `16300`.

10

Deinstalling Oracle WebCenter Content

This chapter explains how to deinstall Oracle WebCenter Content from Oracle Fusion Middleware.

This chapter includes the following sections:

10.1 Preparing to Deinstall Oracle WebCenter Content

Deinstalling Oracle WebCenter Content from your system includes stopping Oracle WebLogic Server, removing application schemas, and deinstalling and removing Oracle homes.

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.

10.2 Stopping Oracle Fusion Middleware

Before deinstalling the Oracle WebCenter Content component from Oracle Fusion Middleware, you should stop all of the servers and processes.

To stop Oracle WebLogic Server and server processes:

1. Stop each Managed Server in the Oracle WebLogic Server domain with the `stopManagedWebLogic` script in the *DomainHome*/bin directory.

   - **UNIX script:** *DomainHome*/bin/stopManagedWebLogic.sh *managedServerName*

   - **Windows script:** *DomainHome*\bin\stopManagedWebLogic.cmd *managedServerName*

   Supply your user name and password when prompted.

2. Close any connections to the Administration Server for the domain, such as a Web browser interface, and stop the Administration Server:

   - **UNIX script:** *DomainHome*/bin/stopWebLogic.sh

   - **Windows script:** *DomainHome*\bin\stopWebLogic.cmd

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

10.3 Removing Oracle WebCenter Content Schemas

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

10.3.1 Starting the Repository Creation Utility

You can download a ZIP file containing the Repository Creation Utility from either of these web sites:

■ Oracle Software Delivery Cloud at

http://edelivery.oracle.com/

■ Oracle Fusion Middleware 11*g* Software Downloads page on Oracle Technology Network (OTN) 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 start RCU as the preceding text describes.

Start RCU with the `rcu` startup file:

■ **UNIX path:** `RCU_HOME`/bin/rcu

■ **Windows path:** `RCU_HOME`\BIN\rcu.bat

10.3.2 Dropping Schemas

Follow these instructions to drop one or more Oracle WebCenter Content 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 WebCenter Content schemas. For more information, see Section 2.2, "Creating Oracle WebCenter Content Schemas with the Repository Creation Utility."

   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 dialog box 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 dialog box, and then click **Next**.

5. Summary screen

   Click **Drop**. A Drop dialog box appears, in which you can click **Stop** before the schemas are dropped.

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

6. Completion Summary screen

   Click **Close**.

10.4 Removing the WebCenter Content Oracle Home

The deinstaller attempts to remove the Oracle home from which it was started. Before you remove the Oracle home for Oracle WebCenter Content, be sure to stop all running processes that use this Oracle home. After you remove the software, you will no longer be able to use your Oracle WebLogic Server domain.

This procedure does not remove any Oracle WebLogic Server domains that you have created. It removes only the software in the WebCenter Content Oracle home.

Follow the instructions in Table 10–1 to deinstall Oracle WebCenter Content.

> **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 10–1   Deinstallation Procedure

No.	Screen	Description and Action Required
1	None	Start the Oracle Fusion Middleware 11*g* WebCenter Content Installer with the `-deinstall` option from the `bin` subdirectory of the `oui` directory in your WebCenter Content Oracle home:
		■ **UNIX command:** *WC_CONTENT_ORACLE_ HOME*`/oui/bin/runInstaller -deinstall`
		■ **Windows command:** *WC_CONTENT_ORACLE_ HOME*`\oui\bin\setup.exe -deinstall`
		On a Windows operating system, you can also start the deinstallation from the **Start** menu by selecting **Programs**, then **Oracle ECM 11g - Home1**, and then **Uninstall**. The names of folders and program groups might be different on your Windows system.
2	Welcome	Click **Next** to continue.
3	Deinstall Oracle Home	Verify the Oracle home you are about to deinstall.
		If you want to save the configuration, click the **Save** button. Then, in the Save dialog box, specify a file, and click **Save**. In the Response File Message dialog box, click **OK**.
		Click **Deinstall** to continue.
4	Deinstallation Progress	This screen shows the progress and status of the deinstallation.
		In the Warning dialog box, click **Yes** to undeploy all Oracle WebCenter Content applications and deinstall Oracle WebCenter content from Oracle Fusion Middleware, or click **No** to undeploy the Oracle WebCenter Content applications without deleting the WebCenter Content Oracle home.
5	Deinstallation Complete	Click **Finish** to dismiss the screen.

10.4.1 Removing the WebCenter Content Oracle Home Manually on a UNIX System

If the deinstallation procedure did not remove your WebCenter Content Oracle home directory, you can use the `rm` command to manually remove the directory and all of its subdirectories on a UNIX operating system.

To remove the WebCenter Content Oracle home on a UNIX operating system:

1. Change directories to the directory that contains the WebCenter Content Oracle home directory:

   ```
   cd MW_HOME
   ```

2. Specify the name of the WebCenter Content Oracle home directory in this command:

   ```
   rm -rf WC_CONTENT_ORACLE_HOME
   ```

10.4.2 Removing the WebCenter Content Oracle Home Manually on a Windows System

If the deinstallation procedure did not remove your WebCenter Content Oracle home directory, you can use the **Delete** command on the **File** menu and remove program groups from the **Start** menu to manually remove the directory and all of its subdirectories on a Windows operating system.

To remove the WebCenter Content Oracle home on a Windows operating system:

- In Windows Explorer, you can navigate to the `C:\`*`MW_HOME`* directory, right-click the *`WC_CONTENT_ORACLE_HOME`* folder, and then choose **Delete** from the **File** menu.

- You can 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 names of folders and program groups might be different on your Windows system.

A
Installation Screens for Oracle WebCenter Content

This appendix describes the Oracle Fusion Middleware 11*g* WebCenter Content Installer screens for installing Oracle WebCenter Content.

This appendix includes the following screens:

- Welcome
- Install Software Updates
- Prerequisite Checks
- Specify Installation Location
- Application Server
- Installation Summary
- Installation Progress
- Installation Complete

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 Install Software Updates
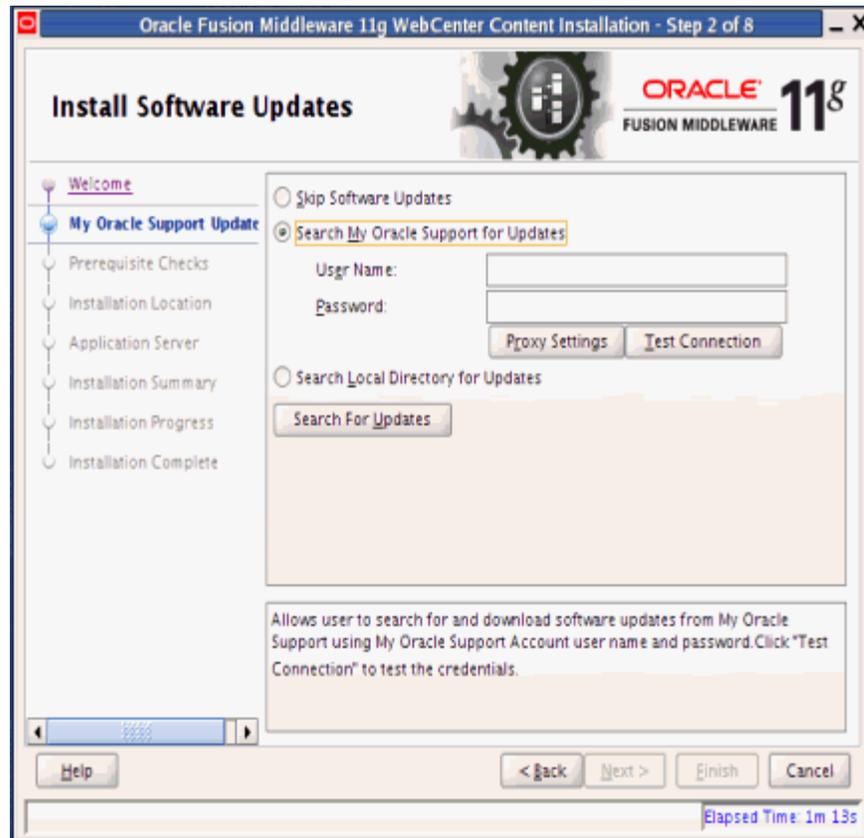
This screen enables you to search for and install software updates before you install Oracle WebCenter Content. The second link on the left is **My Oracle Support Updates** before you make a selection.

To get updates from My Oracle Support, you can select **Search My Oracle Support for Updates**, specify a user name and password, and then click **Search for Updates**. Before you search, you can click **Proxy Settings** to change the settings for the proxy server and **Test Connection** to test the credentials.

To get updates that you have saved to your computer, you can select **Search Local Directory for Updates**, specify a directory, and then click **Search for Updates**.

If you do not want to update any software, you can select **Skip Software Updates**. The link on the left changes from **My Oracle Support Updates** to **Skip Software Updates**.

The **Back** button returns to the Welcome screen.

The **Next** button starts the software updates or continues the installation.

The **Cancel** button stops the installation.

A.3 Prerequisite Checks

This screen shows the prerequisite checks for a Linux 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 previous screen.

The **Next** button continues the installation after the prerequisite checks complete with no errors.

The **Cancel** button stops the installation.

A.4 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 in which to install Oracle WebCenter Content (the WebCenter Content Oracle home directory). This directory must be empty. If the directory does not exist, the installer creates it.

The WebCenter Content Oracle home directory is where all Oracle WebCenter Content 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.5 Application Server

This screen specifies the application server and its location.

The **WebLogic Server** option installs Oracle WebCenter Content on an Oracle WebLogic Server.

The **WebSphere** option installs Oracle WebCenter Content on an IBM WebSphere Application Server. For more information about a WebSphere installation, see "Installing and Configuring Oracle Fusion Middleware on IBM WebSphere" and "Managing Oracle WebCenter Content on IBM WebSphere Application Servers" in the *Oracle Fusion Middleware Third-Party Application Server Guide*.

The **Back** button returns to the previous screen.

The **Next** button continues the installation.

The **Cancel** button stops the installation.

A.6 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.7 Installation Progress

This screen shows you the percentage of progress for the installation.

The **Cancel** button stops the installation before it completes.

A.8 Installation Complete
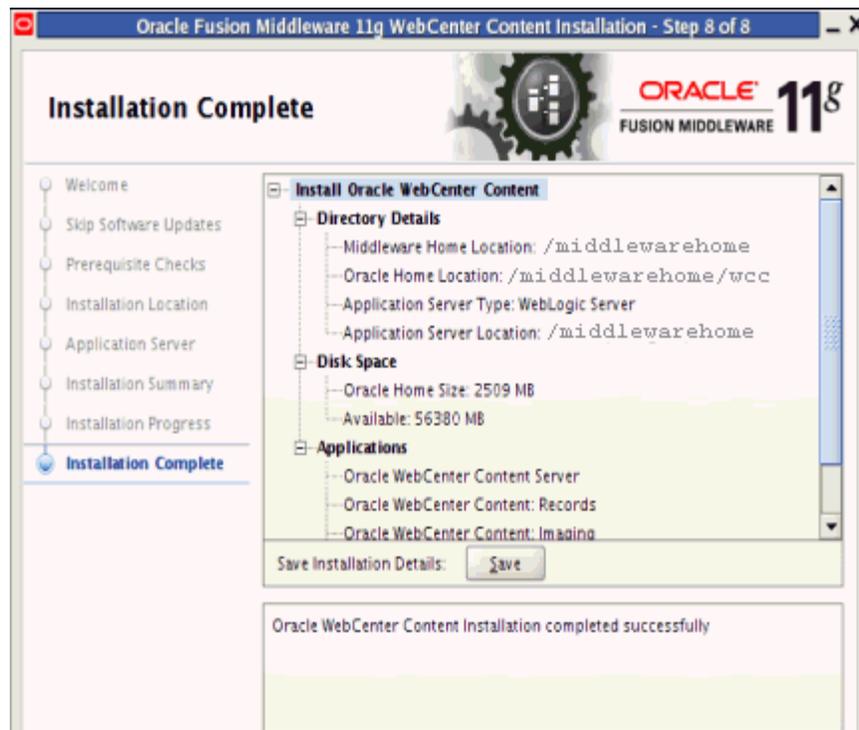
This screen indicates that the installation of Oracle WebCenter Content is complete and summarizes its configuration.

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

Configuration Screens for Oracle WebCenter Content

This appendix describes some Fusion Middleware Configuration Wizard screens for configuring Oracle WebCenter Content applications in an Oracle WebLogic Server domain.

For more information about these and other screens, see "Configuration Wizard Screens" in *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard*.

This appendix includes the following screens:

- Select Domain Source
- Select Extension Source
- Configure JDBC Component Schema
- Configure Managed Servers

For more information about a screen, click the **Help** button on the screen. For more information about configuring Oracle WebLogic Server domains, see *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard*.

B.1 Select Domain Source
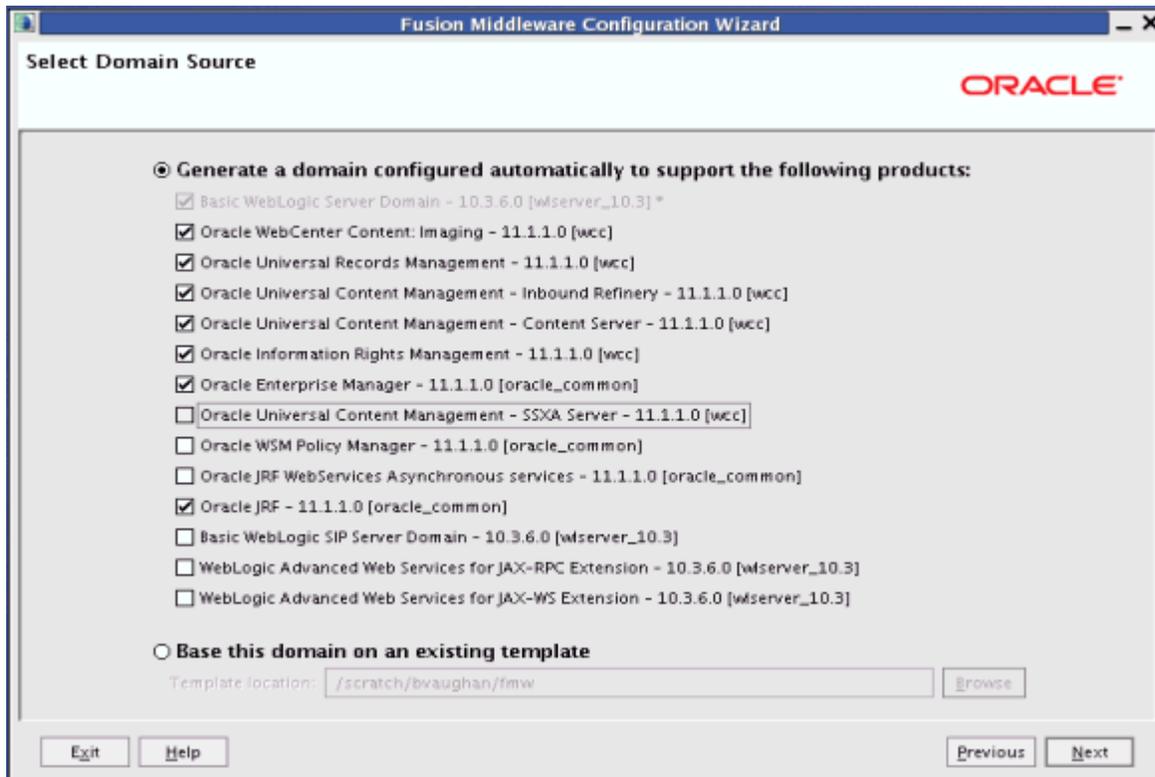
Select **Generate a domain configured automatically to support the following products**, and then select one or more of these product templates:

- **Oracle WebCenter Content: Imaging**

- **Oracle Universal Records Management**

  (for Oracle WebCenter Content: Records)

- **Oracle Universal Content Management - Inbound Refinery**

  (for Oracle WebCenter Content: Inbound Refinery)

- **Oracle Universal Content Management - Content Server**

  (for Oracle WebCenter Content)

- **Oracle Information Rights Management**

When you select **Oracle WebCenter Content: Imaging**, you also need to select **Oracle Universal Content Management - Content Server**, if WebCenter Content is not already configured.

When you select any Oracle WebCenter Content application on the Select Domain Source screen, **Oracle Enterprise Manager** and **Oracle JRF** are automatically selected. If you deselect any of these items that are automatically selected, the Oracle WebCenter Content application will also be deselected.

If you want a remote deployment of a Site Studio for External Applications web site, you can select **Oracle Universal Content Management - SSXA Server** (for Oracle WebCenter Content - SSXA Server) to create an Oracle WebLogic Server domain with a Managed Server that has the files required to run the web site.

To create a domain that includes Oracle Web Services Manager (Oracle WSM) Policy Manager, select **Oracle WSM Policy Manager**.

Alternatively, you can select **Base this domain on an existing template** and then click **Browse** to navigate your directories to find an existing template. For more information, see "Select Domain Source" in *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard*.

Click **Next** to continue.

B.2 Select Extension Source
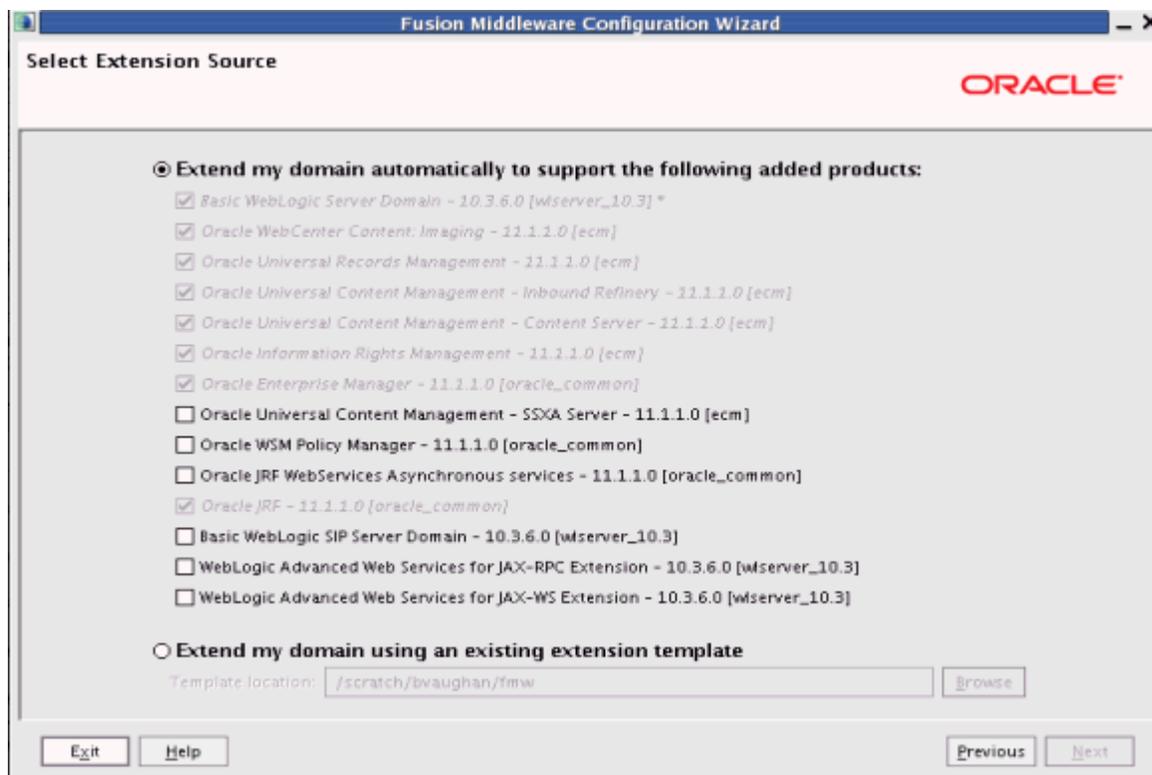
Select the source from which to extend an existing Oracle WebLogic Server domain. Select **Extend my domain automatically to support the following added products**, and then select one or more of the templates that are not already selected.

- **Oracle WebCenter Content: Imaging**

- **Oracle Universal Records Management**

  (for Oracle WebCenter Content: Records)

- **Oracle Universal Content Management - Inbound Refinery**

  (for Oracle WebCenter Content: Inbound Refinery)

- **Oracle Universal Content Management - Content Server**

  (for Oracle WebCenter Content)

- **Oracle Information Rights Management**

When you select **Oracle WebCenter Content: Imaging**, you also need to select **Oracle Universal Content Management - Content Server**, if WebCenter Content is not already configured.

When you select any Oracle WebCenter Content application, **Oracle Enterprise Manager** and **Oracle JRF** are automatically selected. If you deselect any of these items that are automatically selected, the Oracle WebCenter Content application will also be deselected.

If you want a remote deployment for a Site Studio for External Applications web site, you can select **Oracle Universal Content Management - SSXA Server** (for Oracle WebCenter Content - SSXA Server) to extend an Oracle WebLogic Server domain with a Managed Server that has the files required to run the web site.

To extend a domain that includes Oracle Web Services Manager (Oracle WSM) Policy Manager, select **Oracle WSM Policy Manager**.

Alternatively, you can select **Extend my domain using an existing extension template** and specify the path to the extension template in the **Template location** field. For more information, see "Extend Domain Source" in *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard*.

Click **Next** to continue.

B.3 Configure JDBC Component Schema

Use this screen to edit the configuration information for each JDBC component schema. Configure each component schema, including the Oracle WSM MDS schema if it was created with Repository Creation Utility (RCU), by selecting a schema checkbox and then completing 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 or IBM DB2, 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 is 1521 for an Oracle Database instance, `1433` for Microsoft SQL Server, or `50000` for IBM DB2.

Click **Next** to continue.

For more information, see "Configure JDBC Component Schema" in *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard*.

B.4 Configure Managed Servers
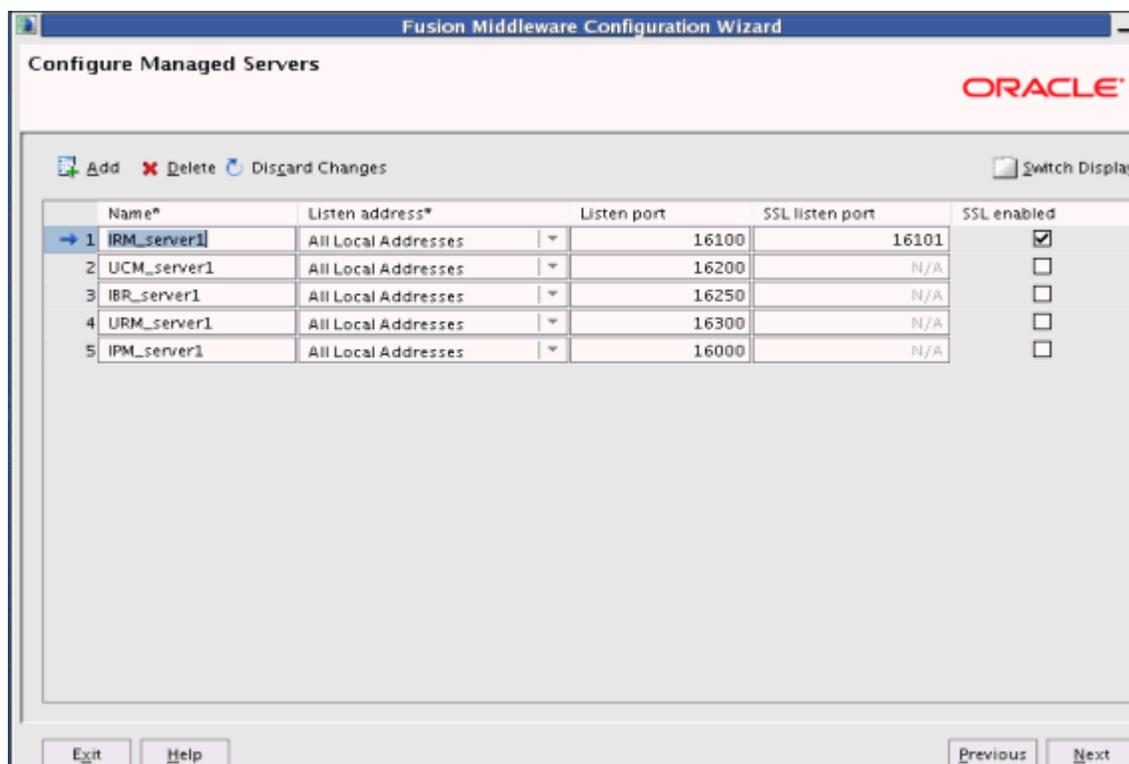
A Managed Server is an instance of Oracle WebLogic Server used to host enterprise applications. A typical production environment has at least one Managed Server.

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.

C

Deinstallation Screens for Oracle WebCenter Content

This appendix describes the Oracle Fusion Middleware 11*g* WebCenter Content Installer screens for deinstalling Oracle WebCenter Content from Oracle Fusion Middleware.

This appendix includes the following screens:

- 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
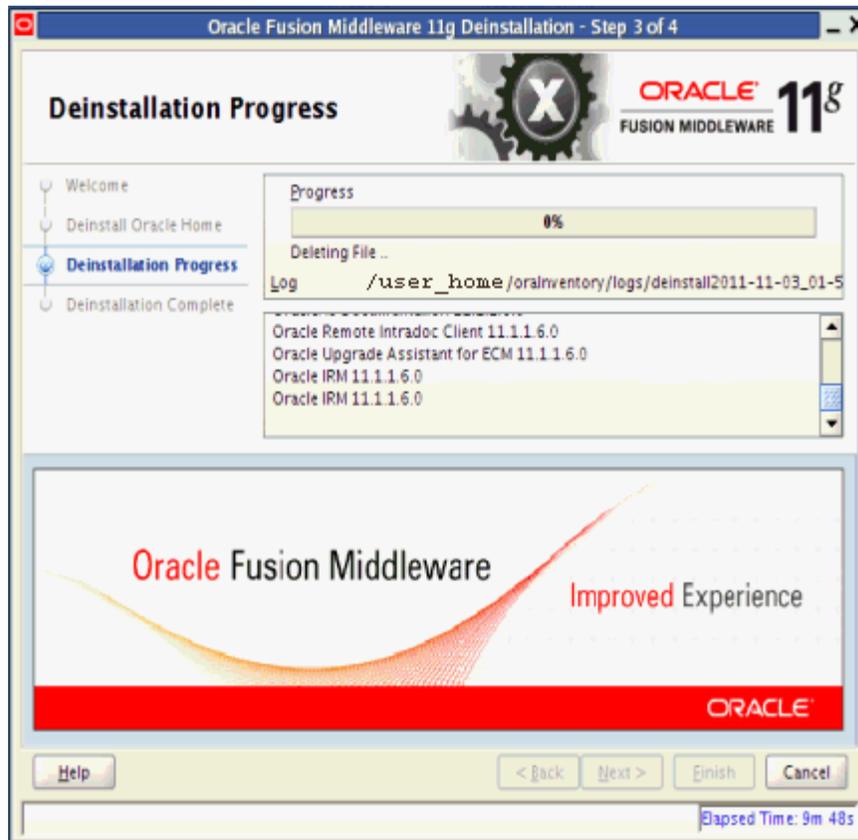
This screen shows you the progress of the deinstallation.

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

Silent Installation

This appendix describes silent installation of Oracle WebCenter Content, without the graphical user interface.

You can install Oracle WebCenter Content from the command line, in silent mode, if you provide a response file with information specific to your installation. When you install Oracle WebCenter Content with the Oracle Fusion Middleware 11*g* WebCenter Content Installer, as described in Section 2.4, "Using the Installer for Oracle WebCenter Content," you can save a response file to perform a silent installation later.

For information about silent installation and deinstallation, see "Silent Installation and Deinstallation" in the *Oracle Fusion Middleware Installation Planning Guide*.

E

Troubleshooting

This appendix provides troubleshooting information.

This appendix includes the following sections:

- Section E.1, "General Troubleshooting Tips"
- Section E.2, "Oracle WebCenter Content Installation and Configuration Troubleshooting"
- Section E.3, "Inbound Refinery Problems"
- Section E.4, "Additional Help"

E.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 2.1.3, "Reviewing System Requirements and Certification".

- 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 10, "Deinstalling Oracle WebCenter Content."

  3. Correct the issue that caused the error.

  4. Restart the installation.

E.2 Oracle WebCenter Content Installation and Configuration Troubleshooting

This section contains solutions to common problems that you might encounter while installing and configuring Oracle WebCenter Content.

If you are having problems with full-text search, Inbound Refinery conversions, Dynamic Converter, Oracle WebCenter Content: Desktop, or Content Categorizer on a Windows operating system, first make sure you have downloaded the correct version of the Visual C++ Redistributable Package, as described in Section 3.7.3, "Downloading Visual C++ Libraries for a Windows Operating System."

E.2.1 Oracle Fusion Middleware Installation and Configuration Log Files

The Oracle Fusion Middleware 11*g* WebCenter Content Installer and Fusion Middleware Configuration Wizard create their own sets of log files.

- On a UNIX operating system, the installer writes the following log files:

    - *oraInventory_location*/logs/installActions*timestamp*.log

    - *oraInventory_location*/logs/oraInstall*timestamp*.err

    - *oraInventory_location*/logs/oraInstall*timestamp*.out

    - *ORACLE_HOME*/install/make.log

- On a Windows operating system, the installer writes the following log files:

    - *inventory_location*\logs\installActions*timestamp*.log

    - *inventory_location*\logs\oraInstall*timestamp*.err

    - *inventory_location*\logs\oraInstall*timestamp*.out

    The default *inventory_location* value follows:

    ```
    %PROGRAMFILES%\Oracle\Inventory
    ```

- Fusion Middleware Configuration Wizard writes log files in the `cfgtoollogs` directory in your Oracle home directory.

If you want to access the log files created by the installer, you need to exit it first. The log files are inaccessible if the installer is still in use.

E.2.2 Oracle IRM Key Store Configuration Issues

If the Oracle Information Rights Management key store has not been configured correctly, then issues will occur during creation of a context. If you cannot create a context, check the server log for one of the following errors.

- Missing key store file

    If the key store does not exist, you will see a `FileNotFoundException` message in the log:

    ```
    java.io.FileNotFoundException: C:\IRM\oracle\middleware\user_projects
    \domains\base_domain\config\fmwconfig\irm.jceks (The system cannot find the
    file specified)
    ```

■   Missing key

   If the key store exists, but the keys are missing, you will see an
   UnknownKeyException message in the log:

```
oracle.irm.engine.content.store.UnknownKeyException:
The key oracle.irm.wrap does not exist in the key store
C:\IRM\oracle\middleware\user_projects\domains\base_
domain\config\fmwconfig\irm.jceks
```

■   Missing password

   If the password is missing or incorrect you will see the following exception in the
   log:

```
java.security.UnrecoverableKeyException: Given final block not properly padded
```

E.2.3 Imaging Errors During Attempt to Connect to WebCenter Content 11g

When you attempt to connect Imaging to a WebCenter Content 11*g* repository,
Imaging returns errors in these cases:

■   If WebCenter Content is installed in a domain that is later extended with Imaging
   and you have not restarted the Imaging Managed Server.

■   If the WebCenter Content and Imaging Managed Servers are configured to run on
   different machines and you have not performed the manual configuration.

For information about avoiding these errors, see Section 6.1.1.1, "Configuring
WebCenter Content 11g to Work with Imaging."

E.3 Inbound Refinery Problems

If you are having problems with Inbound Refinery conversions on a Windows
operating system, first make sure you have downloaded the correct version of the
Visual C++ Redistributable Package, as described in Section 3.7.3, "Downloading
Visual C++ Libraries for a Windows Operating System."

This section provides troubleshooting information for the following Inbound Refinery
setup and run issues:

■   Inbound Refinery Will Not Run As an Application or Service

■   Inbound Refinery Runs As an Application But Not As a Service

■   Inbound Refinery Service Keeps Stopping

■   Cannot Log In to Refinery After Installation

■   Files Intermittently Stuck in GenWWW Status

■   Inbound Refinery Service Will Not Convert Documents

E.3.1 Inbound Refinery Will Not Run As an Application or Service

Inbound Refinery will not run as either an application or a service. If you try to run
Inbound Refinery from a command line, you receive the following error message:

```
Error: Cannot read the config.cfg.
```

Possible Causes	Solutions
Sun Java is not installed on the Inbound Refinery machine. Sun Java must be installed on both the Content Server machine and the Inbound Refinery machine.	■ Reinstall Inbound Refinery to reinstall the Sun JVM.
	■ Copy the Sun Java files from the Content Server machine to the Inbound Refinery machine. Open the `intradoc.cfg` file located in the `refinery_install_dir`\bin directory and make sure the `JAVA_EXE` path is correct.
	■ Another option is to download a copy of Sun Java from the Downloads page on the Sun Developer Network web site at
	http://www.oracle.com/technetwork/indexes/downloads/index.html
	Install it on the Inbound Refinery machine. Open the `intradoc.cfg` file located in the `refinery_install_dir`\bin directory and make sure the `JAVA_EXE` path is correct.

E.3.2 Inbound Refinery Runs As an Application But Not As a Service

Inbound Refinery will run as an application, but it will not run as a service. In some cases, you will receive the following error message when launching the service:

```
Error 1069: The service did not start due to a logon failure.
```

Possible Causes	Solutions
If you receive Error 1069, the user linked to the Inbound Refinery service has not been given the right to log on as a service.	Make sure user linked to the Inbound Refinery service is valid and has the right to log on as a service.
There is a problem with the Inbound Refinery service.	■ Reboot the Inbound Refinery machine.
	■ Try running Inbound Refinery as an application, then retry running it as a service. Sometimes running Inbound Refinery as an application once will clear up problems with the service.
	■ Delete and re-add the service in Inbound Refinery.

E.3.3 Inbound Refinery Service Keeps Stopping

The Inbound Refinery service will run for a short period of time when started, but then the service fails and stops.

Possible Causes	Solutions
Java options settings in the `intradoc.cfg` file for the refinery.	Change the Java options settings in the `intradoc.cfg` file for the Inbound Refinery connection.

To set up Java options in the intradoc.cfg file:

1. Open the `intradoc.cfg` file located in the *refinery_install_dir*\bin directory in a text editor.

2. First, try the following setting:

   ```
   JAVA_SERVICE_EXTRA_OPTIONS=-Xrs
   ```

3. Save your changes to the `intradoc.cfg` file and restart the Inbound Refinery service.

4. If the first change is not successful, re-open the `intradoc.cfg` file and try the following setting:

   ```
   JvmCommandLine=$JAVA_EXE $JAVA_SERVICE_EXTRA_OPTIONS $APPEND_CLASSPATH
   $CLASSPATH $STARTUPCLASS
   ```

5. Save your changes to the `intradoc.cfg` file and restart the Inbound Refinery service.

E.3.4 Cannot Log In to Refinery After Installation

When you attempt to log in to a refinery after installation, you get an error similar to the following one:

```
"Content Server Access Denied
Access denied to Content Server managed resource. Error getting user credentials
from proxied user cache. Unable to open file
c:/ucm/cs1/data/users/proxied/ref1/userdb.txt.
 c:/ucm/cs1/data/users/proxied/ref1/userdb.txt contains an invalid path."
```

Possible Causes	Solutions
The refinery has been proxied to Content Server, but the InboundRefinerySupport component has not been installed and enabled on Content Server.	Install and enable the InboundRefinerySupport component on Content Server.
	For more information, see Section 5.2.3.2, "Enabling Components for Inbound Refinery on Content Server."

E.3.5 Files Intermittently Stuck in GenWWW Status

When WebCenter Content is run on a Windows Server 2003 system, files intermittently get stuck in GenWWW. There are no conversion errors, and when resubmitted, the files are successfully converted.

Possible Causes	Solutions
The problem is directly related to known file locking and deleting issues on a Windows Server 2003 system and typically occurs when Content Server runs on a UNIX operating system and Samba is used to connect to the Windows Server 2003 machine. However, the problem can also occur when you are using Inbound Refinery on the Windows Server 2003 system and Inbound Refinery resides on a separate physical machine from Content Server. For more information about these Windows Server 2003 issues, see knowledge base articles 885451 and 811492 on the Microsoft Support web site at http://support.microsoft.com	To confirm that you are experiencing the issues described in Microsoft's knowledge base articles, delete several files on your Windows Server 2003 machine using a remote client. If you witness a delay of up to 40 seconds in the file deletion, it is likely that the Windows Server 2003 locking/deleting issue is the problem. Microsoft offers two solutions to this issue. **1.** Microsoft has a hotfix for Windows Server 2003 that can be shipped on a request-only basis. However, Microsoft's recommendation is to wait until the next service pack unless you are 'severely' affected by the problem. **2.** The alternate solution from Microsoft is to disable *opportunistic locking* on the Windows Server 2003 server. The solution to disable opportunistic locking does not impact the normal file locking used when writing a file. Rather, opportunistic locking is a speed tweak to the file locking process that can be safely disabled if it is causing problems. Additional information on opportunistic locks is contained in the Samba help files. If you need specific information on how to disable opportunistic locking on a Windows Server 2003 server, see knowledge base article 29624 on the Microsoft Support web site at http://support.microsoft.com

E.3.6 Inbound Refinery Service Will Not Convert Documents

You are running Inbound Refinery as a service, but it will not convert any documents, and the following error message is displayed in the Inbound Refinery log:

```
Unable to convert, native application reported: 'Permission denied'
```

This error will usually occur when Samba is used with Content Server on a UNIX operating system or with Inbound Refinery on a Windows operating system.

Possible Causes	Solutions
You are using AutoExNT to map the UNIX volumes through a mapped network drive to Samba, and the DCOM permissions are not set properly for the user running the Inbound Refinery service.	Change the DCOM permissions for the user running the Inbound Refinery service. For details, see the following procedure for changing DCOM permissions.

To change DCOM permissions:

1. Launch dcmocnfg.exe to check user permissions for the user running the Inbound Refinery service.

2. On the **Default Security** tab, make sure the domain user is added to **Connect**, **Access**, **Launch**, and **Configuration**.

3. Restart the Inbound Refinery service.

E.4 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