

Oracle® Fusion Middleware

Installation Guide for Oracle Enterprise Content Management
Suite

11g Release 1 (11.1.1)

E14495-04

January 2011

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

E14495-04

Copyright © 1996, 2011, Oracle and/or its affiliates. All rights reserved.

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, Alex Barnett, Pete Chapman, Sandra Christiansen, Eric Cloney, Rupesh Das, Carl Foster, Sudhanshu Garg, Brian Gray, Helen Grembowicz, Marsha Hancock, Mary Hoepner, Mei Hong, David Jones, Vasant Kumar, Peter LaQuerre, Bill Loi, Rene Madsen, Liju Nair, John Neely, Saskia Nehls, Bob O'Kane-Trombley, Toby O'Sullivan, Jason Ogaard, 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

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

Preface	ix
Audience.....	ix
Documentation Accessibility.....	ix
Related Documents.....	x
Conventions.....	x
1 Installation Overview	
1.1 Oracle Enterprise Content Management Suite Applications.....	1-1
1.2 Software Downloads for Oracle ECM Installation and Configuration.....	1-2
1.2.1 Downloading Software from Oracle E-Delivery for Installing and Configuring Oracle ECM.....	1-2
1.2.2 Downloading Software from OTN for Installing and Configuring Oracle ECM.....	1-3
1.3 Installation Roadmap.....	1-3
1.4 Installation Modules.....	1-7
1.4.1 Oracle Fusion Middleware and Oracle WebLogic Server Homes.....	1-7
1.4.2 Database.....	1-8
1.4.3 Repository Creation Utility.....	1-8
1.4.4 Oracle Enterprise Content Management Suite.....	1-8
1.5 Oracle WebLogic Server Domain.....	1-9
1.6 Directory Structure for Oracle Enterprise Content Management Suite.....	1-9
2 Creating Schemas for Oracle Enterprise Content Management Suite	
2.1 Preparing to Run Repository Creation Utility and Load Schemas.....	2-1
2.1.1 Database Prerequisites.....	2-1
2.1.2 RCU for Linux and Windows Operating Systems.....	2-2
2.2 Creating Oracle Enterprise Content Management Suite Schemas.....	2-2
3 Installing Oracle Enterprise Content Management Suite	
3.1 Preparing for Installation.....	3-1
3.1.1 Meeting System Requirements.....	3-1
3.1.2 Installing Oracle WebLogic Server in a Middleware Home.....	3-2
3.1.3 Install and Configure Java Access Bridge (Windows Operating System Only).....	3-4
3.1.4 Configure a DHCP Host.....	3-5
3.1.4.1 Configuring a DHCP Host on a UNIX Operating System.....	3-5
3.1.4.2 Configuring a DHCP Host on a Windows Operating System.....	3-5

3.1.4.3	Installing a Loopback Adapter on a Windows Operating System.....	3-5
3.1.4.4	Removing a Loopback Adapter from a Windows Operating System.....	3-6
3.1.5	Installing on a Non-Networked Computer	3-7
3.1.6	Installing on a Multihomed Computer.....	3-7
3.2	Installing Oracle Enterprise Content Management Suite in Oracle Fusion Middleware.	3-7
3.2.1	Creating a Symbolic Link to the chmod Command on a Solaris System	3-8
3.2.2	Locating Installation Log Files.....	3-8
3.2.3	Starting the Installer	3-8
3.2.4	Providing the Location of the Inventory Directory on a UNIX System	3-9
3.2.5	Installing Oracle Enterprise Content Management Suite	3-9

4 Configuring Oracle Enterprise Content Management Suite

4.1	Preparing to Configure Oracle Enterprise Content Management Suite	4-1
4.2	Creating an Oracle WebLogic Server Domain.....	4-3
4.3	Extending an Existing Domain	4-10
4.4	Extending a Domain in an SSL Environment	4-15
4.5	Increasing the Java VM Heap Size for Managed Servers.....	4-16
4.5.1	Setting Server Startup Parameters for Managed Servers with the Administration Console	4-16
4.5.2	Setting the USER_MEM_ARGS Environment Variable for a Managed Server.....	4-17
4.6	Setting Up Fonts on a UNIX System	4-18
4.6.1	Setting Up TrueType Fonts on a UNIX System.....	4-18
4.6.2	Installing Fonts for National Language Support on a UNIX System.....	4-19
4.7	Installing Libraries and Setting Environment Variables for Outside In Technology	4-19
4.7.1	Installing Libraries for Outside In Technology on UNIX Platforms.....	4-19
4.7.2	Setting Library Paths in Environment Variables on UNIX Platforms	4-22
4.7.3	Downloading Visual C++ Libraries for a Windows Operating System.....	4-22
4.8	Configuring SSL for Oracle ECM Applications.....	4-23
4.8.1	Configuring SSL for a Production Environment.....	4-23
4.8.2	Configuring SSL for a Development Environment	4-23
4.8.2.1	Configuring One-Way SSL for a Development Environment	4-24
4.8.2.2	Configuring Clients to Accept the Server Certificate	4-26
4.9	Reassociating the Identity Store with an External LDAP Authentication Provider	4-27
4.9.1	Reassociating the Identity Store with Oracle Internet Directory	4-27
4.9.2	Refreshing GUID Values in Oracle I/PM Security Tables	4-33
4.9.2.1	Refreshing GUID values in Oracle I/PM Security Tables with WLST.....	4-34
4.9.2.2	Refreshing GUID values in Oracle I/PM Security Tables with Fusion Middleware Control.....	4-34
4.10	Adding Users to Oracle Internet Directory	4-35
4.11	Installing Fonts for National Language Support on a UNIX System.....	4-36
4.12	Configuring Single Sign-On (SSO)	4-37
4.12.1	Configuring Oracle Access Manager Single Sign-On.....	4-37
4.12.2	Configuring Oracle Single Sign-On	4-38
4.12.3	Configuring Windows Native Authentication.....	4-39
4.13	Configuring Managed Server Clusters	4-39

4.14	Setting Up Oracle Web Services Manager Security	4-40
4.14.1	Installing Oracle WebLogic Server and Oracle Enterprise Content Management Suite	4-41
4.14.2	Creating an Oracle WSM MDS Schema with RCU.....	4-41
4.14.3	Configuring Oracle ECM Applications and Oracle WSM Policy Manager in an Oracle WebLogic Server Domain	4-41
4.14.4	Configuring the Server Socket Port and Incoming Socket Connection Address Security Filter for Oracle WSM.....	4-41
4.14.5	Securing Web Services with a Key Store and Oracle WSM Policies	4-42
4.14.5.1	Setting Up a Key Store	4-42
4.14.5.2	Applying Oracle WSM Policies to Web Services	4-43

5 Configuring Oracle Universal Content Management

5.1	Completing the Oracle UCM Configuration.....	5-1
5.2	Completing the Initial Configuration of Oracle Content Server.....	5-3
5.2.1	Starting Oracle Content Server	5-3
5.2.2	Configuring the Oracle Content Server Instance	5-3
5.2.3	Enabling or Disabling Components	5-7
5.2.4	Configuring Oracle Content Server for IBM DB2 Database Searches.....	5-7
5.2.5	Configuring Microsoft SQL Server to Work with Oracle UCM.....	5-7
5.3	Configuring Oracle Text Search for Oracle Content Server	5-8
5.3.1	Applying Patches for Using Oracle Text 11g with Oracle Database 11.1.0.7.0.....	5-9
5.3.2	Configuring an External Database Provider for Standalone Applications	5-10
5.4	Configuring a JDBC Driver for Standalone Applications.....	5-10
5.5	Importing a Database Root CA Certificate into the Key Store for a Standalone Application	5-12
5.6	Enabling and Configuring Site Studio on Oracle Content Server	5-12
5.6.1	Enabling Site Studio on Oracle Content Server.....	5-13
5.6.2	Setting Default Project Document Information.....	5-14
5.6.3	Setting Default Metadata for Web Site Assets.....	5-14
5.6.4	Configuring Zone Fields.....	5-14
5.6.5	Enabling JavaServer Pages on Oracle Content Server.....	5-15
5.6.6	Rebuilding the Oracle Content Server Index.....	5-16
5.7	Configuring Oracle Content Server for Desktop Integration Suite	5-16
5.8	Installing and Configuring Desktop Integration Suite on a Client Workstation.....	5-17
5.9	Opening Files from Microsoft Office 2010 Over a Non-SSL Connection	5-17
5.10	Configuring Records Management in Oracle Content Server	5-17
5.11	Configuring Oracle Application Extension Framework	5-19
5.12	Installing and Configuring Oracle Document Capture and Oracle Distributed Document Capture	5-20

6 Configuring Oracle Inbound Refinery

6.1	Completing the Oracle IBR Configuration.....	6-1
6.2	Installing and Configuring Oracle IBR on Oracle UCM	6-2
6.2.1	Configuring Oracle IBR on Oracle UCM.....	6-2

6.2.2	Configuring Document Conversion on Oracle IBR.....	6-5
6.2.2.1	Enabling Conversion Components on Oracle IBR	6-5
6.2.2.2	Enabling PDFExportConverter in Oracle IBR.....	6-5
6.2.3	Setting Up Oracle Content Server to Send Jobs to Oracle IBR for Conversion	6-6
6.2.3.1	Creating an Outgoing Provider.....	6-6
6.2.3.2	Enabling Components for Oracle IBR on Oracle Content Server.....	6-7
6.2.3.3	Selecting File Formats To Be Converted	6-8

7 Configuring Oracle Imaging and Process Management

7.1	Completing the Oracle I/PM Configuration	7-1
7.1.1	Configuring an Oracle UCM Repository for Oracle I/PM.....	7-2
7.1.1.1	Configuring Oracle Content Server 11g to Work with Oracle I/PM.....	7-2
7.1.1.2	Installing and Configuring Oracle UCM 10g to Work with Oracle I/PM.....	7-3
7.1.1.3	Configuring a File Store Provider for Content Storage.....	7-6
7.1.2	Starting the Oracle I/PM Managed Server and Accessing the Web Client	7-7
7.1.3	Connecting to an Oracle UCM Repository	7-7
7.1.4	Configuring the GDFontPath MBean for a UNIX System.....	7-8
7.1.5	Allowing IMPORT Definitions	7-9
7.2	Configuring the Full-Text Features in the Oracle UCM Repository	7-10
7.3	Connecting to a Workflow Server	7-10
7.4	Setting Oracle I/PM System Security	7-10
7.5	Installing and Configuring Oracle Application Extension Framework.....	7-11
7.5.1	Configuring the Java Object Cache for AXF in Distributed Oracle I/PM Managed Servers	7-11
7.5.2	Verifying the AXF Installation with HelloWorld.....	7-12
7.5.3	Verifying the AXF Installation with HelloBpel	7-13
7.6	Installing and Configuring Oracle Document Capture and Oracle Distributed Document Capture	7-15

8 Configuring Oracle Information Rights Management

8.1	Performing Postinstallation Configuration.....	8-1
8.1.1	Setting the Server URL Configuration Parameter for Oracle IRM.....	8-1
8.1.2	Configuring a Key Store for Oracle IRM.....	8-2
8.1.2.1	Choosing a Cryptographic Algorithm, Key Size, and Key Store	8-3
8.1.2.2	Creating a Key Store	8-3
8.1.2.3	Setting the Key Store Location.....	8-4
8.1.2.4	Adding Key Store Passwords to the Credential Store	8-6
8.1.2.5	Configuring the Policy and Credential Store	8-7
8.2	Validating the Oracle IRM Installation.....	8-8
8.3	Configuring the Identity Store	8-8
8.4	Integrating Oracle IRM with Oracle Access Manager 11g.....	8-8

9 Configuring Oracle Universal Records Management

9.1	Completing the Oracle URM Configuration.....	9-1
9.1.1	Enabling Oracle URM Components.....	9-1
9.1.2	Completing the Setup Checklist for Oracle URM.....	9-3

9.2	Using Oracle Text Search with Oracle URM.....	9-6
9.3	Setting Connection Pool Property Values for an IBM DB2 Data Source	9-7
9.4	Installing and Configuring Desktop Integration Suite on a Client Workstation.....	9-7

10 Verifying the Installation and Configuration

10.1	Starting the Administration Server	10-1
10.2	Starting Managed Servers.....	10-2
10.3	Restarting a Managed Server	10-4
10.4	Starting Node Manager.....	10-5
10.5	Increasing the Java Heap Size for a Managed Server	10-6
10.6	Verifying the Installation	10-6

11 Deinstalling Oracle Enterprise Content Management Suite

11.1	Introduction to Deinstalling Oracle Enterprise Content Management Suite.....	11-1
11.2	Stopping Oracle WebLogic Server and Server Processes.....	11-1
11.3	Removing Oracle Enterprise Content Management Suite Schemas	11-2
11.3.1	Starting Repository Creation Utility	11-2
11.3.2	Dropping Schemas.....	11-3
11.4	Deinstalling the ECM Oracle Home.....	11-3
11.5	Removing Oracle Home Directories Manually	11-4

A Oracle Enterprise Content Management Suite Installation Screens

A.1	Welcome	A-2
A.2	Install Software Updates	A-3
A.3	Prerequisite Checks	A-4
A.4	Specify Installation Location	A-5
A.5	Installation Summary	A-6
A.6	Installation Progress	A-7
A.7	Installation Completed.....	A-8

B Oracle Enterprise Content Management Suite Configuration Screens

B.1	Welcome	B-2
B.2	Select a WebLogic Domain Directory	B-3
B.3	Select Domain Source	B-4
B.4	Select Extension Source	B-5
B.5	Specify Domain Name and Location	B-6
B.6	Configure Administrator User Name and Password	B-7
B.7	Configure Server Start Mode and JDK	B-8
B.8	Configure JDBC Component Schema	B-9
B.9	Test Component Schema	B-10
B.10	Select Optional Configuration.....	B-11
B.11	Configure the Administration Server	B-12
B.12	Configure Managed Servers.....	B-13
B.13	Configure Clusters.....	B-14
B.14	Assign Servers to Clusters	B-15

B.15	Create HTTP Proxy Applications	B-15
B.16	Configure Machines.....	B-16
B.17	Assign Servers to Machines.....	B-17
B.18	Target Deployments to Clusters or Servers	B-18
B.19	Target Services to Clusters or Servers.....	B-19
B.20	Select JMS Distributed Destination Type	B-20
B.21	Configure RDBMS Security Store Database.....	B-21
B.22	Configure JMS File Stores	B-22
B.23	Configuration Summary	B-23
B.24	Creating Domain.....	B-24
B.25	Extending Domain.....	B-25

C Deinstallation Screens

C.1	Welcome	C-2
C.2	Deinstall Oracle Home	C-3
C.3	Deinstallation Progress	C-4
C.4	Deinstallation Complete	C-5

D Troubleshooting

D.1	General Troubleshooting Tips	D-1
D.2	Suite Installation and Configuration Troubleshooting	D-2
D.2.1	Oracle Fusion Middleware Installation and Configuration Log Files	D-2
D.2.2	Oracle IRM Key Store Configuration Issues	D-2
D.2.3	Oracle I/PM Errors During Attempt to Connect to Oracle UCM 11g.....	D-3
D.3	Oracle Inbound Refinery Problems.....	D-3
D.3.1	Oracle IBR Will Not Run As an Application or Service.....	D-3
D.3.2	Oracle IBR Runs As an Application But Not As a Service	D-4
D.3.3	Oracle IBR Service Keeps Stopping.....	D-4
D.3.4	Cannot Log In to Refinery After Installation	D-5
D.3.5	Files Intermittently Stuck in GenWWW Status	D-5
D.3.6	Oracle IBR Service Will Not Convert Documents.....	D-6
D.4	Additional Help	D-7

Index

Preface

This installation guide provides information and instructions for installing, configuring, and troubleshooting Oracle Enterprise Content Management Suite.

Audience

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

Documentation Accessibility

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/support/contact.html> or visit <http://www.oracle.com/accessibility/support.html> 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 Conversion*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Application Adapters for Oracle Enterprise Content Management*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*
- *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter*
- *Oracle Fusion Middleware Application Security Guide*
- *Oracle Fusion Middleware Concepts*
- *Oracle Fusion Middleware E-Business Suite Adapter for Oracle Enterprise Content Management Administrator's Guide*
- *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Enterprise Content Management Suite*
- *Oracle Fusion Middleware High Availability Guide*
- *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*
- *Oracle Fusion Middleware Installation Planning Guide*
- *Oracle Fusion Middleware Node Manager Administrator's Guide for Oracle WebLogic Server*
- *Oracle Fusion Middleware Quick Installation Guide for Oracle Enterprise Content Management Suite*
- *Oracle Fusion Middleware Repository Creation Utility User's Guide*
- *Oracle Fusion Middleware Securing Oracle WebLogic Server*
- *Oracle Fusion Middleware Using Clusters for Oracle WebLogic Server*
- *Oracle Fusion Middleware User's Guide for Desktop Integration Suite*
- *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*

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.
<i>italic</i>	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.

Installation Overview

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

- [Oracle Enterprise Content Management Suite Applications](#)
- [Software Downloads for Oracle ECM Installation and Configuration](#)
- [Installation Roadmap](#)
- [Installation Modules](#)
- [Oracle WebLogic Server Domain](#)
- [Directory Structure for Oracle Enterprise Content Management Suite](#)

1.1 Oracle Enterprise Content Management Suite Applications

Oracle Enterprise Content Management Suite includes the following products:

- **Oracle Universal Content Management (Oracle UCM)**

Oracle UCM, which includes Oracle Content Server, provides a unified application for several different types of content management.
- **Oracle Inbound Refinery (Oracle IBR)**

Oracle IBR is a conversion server that manages file conversions for electronic assets such as documents, digital images, and motion video. In addition to conversion, Oracle IBR 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 Oracle IBR to convert content items stored in Oracle Content Server.
- **Oracle Imaging and Process Management (Oracle I/PM)**

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

- **Oracle Information Rights Management (Oracle IRM)**

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

- **Oracle Universal Records Management (Oracle URM)**

Oracle URM manages content items on a retention schedule, which determines the life cycle of each content item. Oracle URM combines both records management and retention management into one software system. You can use Oracle URM 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 ECM 11.1.1.4.0 application in an Oracle WebLogic Server domain that already has an Oracle ECM application from an earlier release installed.

1.2 Software Downloads for Oracle ECM Installation and Configuration

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

- Oracle E-Delivery
- Oracle Technology Network (OTN)

1.2.1 Downloading Software from Oracle E-Delivery for Installing and Configuring Oracle ECM

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

To download software from Oracle E-Delivery for installing and configuring Oracle ECM

1. Go to the Oracle E-Delivery 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 11.1.1.4.0, which includes Oracle ECM.
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 Downloading Software from OTN for Installing and Configuring Oracle ECM

You can download Oracle WebLogic Server 11gR1 (10.3.4), Oracle Database, Repository Creation Utility, and Oracle ECM software from Oracle Technology Network (OTN).

To download software from OTN for installing and configuring Oracle ECM

1. If you do not have Oracle WebLogic Server 11gR1 (10.3.4) 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/index.html>

Download Oracle WebLogic Server 11gR1 (10.3.4) 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.html>

Download Oracle Database 11g 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 Enterprise Content Management Suite, 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 Enterprise Content Management Suite media and the corresponding version of Repository Creation Utility, go to the Oracle Fusion Middleware 11g Software Downloads page on OTN at

http://www.oracle.com/technology/software/products/middleware/htdocs/fmw_11_download.html

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

- **SOA Suite (11.1.1.4.0)** under Runtime Software
- **JDeveloper and Application Development Framework (11.1.1.4.0)** 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 Installation Roadmap

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

Table 1–1 Oracle Enterprise Content Management Suite Installation Procedure

Task	Description	Mandatory/ Optional?	Documentation
Task 1 - Prepare your system environment for installation	Ensure that your system environment meets the general installation requirements for Oracle Fusion Middleware, for Oracle Enterprise Content Management Suite, and for Repository Creation Utility (RCU), which requires a supported database.	Mandatory	Section 3.1, "Preparing for Installation."
Task 2 - Create schemas for applications	<p>Oracle Enterprise Content Management Suite 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 Enterprise Content Management Suite schemas, then install RCU and use it to create schemas.</p> <p>Note: You can perform this task before or after Task 3 - Install Oracle WebLogic Server in a Middleware home and Task 4 - Install Oracle Enterprise Content Management Suite.</p>	Mandatory	Section 1.4.2, "Database" Chapter 2, "Creating Schemas for Oracle Enterprise Content Management Suite"
Task 3 - Install Oracle WebLogic Server in a Middleware home	<p>Oracle Enterprise Content Management Suite runs on Oracle WebLogic Server. You must install Oracle WebLogic Server before you install Oracle Enterprise Content Management Suite.</p> <p>The installer creates the Oracle WebLogic Server home directory (<i>WL_HOME</i>) within the Middleware home directory (<i>MW_HOME</i>).</p> <p>Note: You can perform this task before or after Task 2 - Create schemas for applications.</p>	Mandatory	Section 3.1.2, "Installing Oracle WebLogic Server in a Middleware Home"

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

Task	Description	Mandatory/ Optional?	Documentation
Task 4 - Install Oracle Enterprise Content Management Suite	<p>Use the Oracle Fusion Middleware 11g Oracle Enterprise Content Management Suite Installer to install Oracle Enterprise Content Management Suite. Within the Middleware home, the installer creates an Oracle home directory named <code>Oracle_ECM</code>, where it installs the Oracle Enterprise Content Management Suite products.</p> <p>The installer lays down the Oracle Enterprise Content Management Suite binaries for these products:</p> <ul style="list-style-type: none"> ■ Oracle I/PM ■ Oracle IRM ■ Oracle UCM ■ Oracle URM ■ Oracle IBR <p>Note: You can perform this task before or after Task 2 - Create schemas for applications, but you need to perform it after Task 3 - Install Oracle WebLogic Server in a Middleware home.</p>	Mandatory	Chapter 3, "Installing Oracle Enterprise Content Management Suite"
Task 5 - Configure Oracle Enterprise Content Management Suite	<p>Create or extend an Oracle WebLogic Server domain and choose the products that you want to deploy and configure as applications.</p> <p>Fusion Middleware Configuration Wizard creates an Oracle WebLogic Server domain, which contains the Administration Server and one or more Managed Servers, such as <code>IRM_server1</code>, depending on the products that you choose.</p> <p>After you have created a domain, you can later extend that domain to deploy and configure additional Oracle Enterprise Content Management Suite products as applications.</p>	Mandatory	Chapter 4, "Configuring Oracle Enterprise Content Management Suite"

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

Task	Description	Mandatory/ Optional?	Documentation
Task 6 - Install and configure an external LDAP-based identity store	<p>By default, Oracle Enterprise Content Management Suite uses the Oracle WebLogic Server embedded LDAP server. Although secure, the out-of-the-box embedded LDAP may not scale appropriately for enterprise production environments.</p> <p>In a production system, Oracle Enterprise Content Management Suite applications need to use an external Lightweight Directory Application Protocol (LDAP) authentication provider rather than the Oracle WebLogic Server embedded LDAP server. 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.</p> <p>Note: If you perform this task before Task 8 - Perform Postinstallation Configuration and Task 7 - Verify the installation, the postinstallation configuration is easier.</p>	Optional	Section 4.9, "Reassociating the Identity Store with an External LDAP Authentication Provider."
Task 7 - Verify the installation	<p>To verify the installation, you can start the Administration Server and Managed Servers.</p> <p>Before you can start a Managed Server the first time, you must start the Administration Server.</p> <p>To start working with an Oracle Enterprise Content Management Suite application, you must start the Managed Server to which that application is deployed. You can then access the application's URL and complete the configuration according to your requirements.</p>	Mandatory	Chapter 10, "Verifying the Installation and Configuration"
Task 8 - Perform Postinstallation Configuration	<p>For each Oracle Enterprise Content Management Suite application, you need to perform some initial configuration to get the application up and running in the Managed Server. Some of this initial configuration needs to be done before you start the Managed Server for the first time.</p>	Mandatory	Chapter 5, "Configuring Oracle Universal Content Management" Chapter 6, "Configuring Oracle Inbound Refinery" Chapter 7, "Configuring Oracle Imaging and Process Management" Chapter 8, "Configuring Oracle Information Rights Management" Chapter 9, "Configuring Oracle Universal Records Management"

1.4 Installation Modules

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

- [Oracle Fusion Middleware and Oracle WebLogic Server Homes](#)
- [Database](#)
- [Repository Creation Utility](#)
- [Oracle Enterprise Content Management Suite](#)

1.4.1 Oracle Fusion Middleware and Oracle WebLogic Server Homes

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

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

```
/middleware_home
  coherence_3.6
  jdk160_21
  jrockit_160_20_1.1.0-2119
  logs
  modules
  wlserver_10.3
  oracle_common
  utils
  ECM_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 Oracle Middleware home is `/Oracle/Middleware` on a UNIX operating system or `\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 *Oracle Fusion Middleware Installation Planning Guide*.

The ECM Oracle home contains the binary and library files necessary for Oracle Enterprise Content Management Suite. `ECM_ORACLE_HOME` represents the ECM Oracle home in path names. The default ECM Oracle home is `MW_HOME/Oracle_ECM1` on a UNIX operating system or `MW_HOME\Oracle_ECM1` on a Windows operating system.

The ECM Oracle home can be associated with multiple Oracle WebLogic Server domains. The Oracle Common home contains the binary and library files required for Oracle Enterprise Manager 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 *Oracle Fusion Middleware Administrator's Guide*.

1.4.2 Database

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

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

Note: RCU is available only 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.

The overall performance of an Oracle UCM 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 the latest information about supported databases, see the Oracle Fusion Middleware Supported System Configurations page on Oracle Technology Network at

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

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

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

1.4.3 Repository Creation Utility

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

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

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

1.4.4 Oracle Enterprise Content Management Suite

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

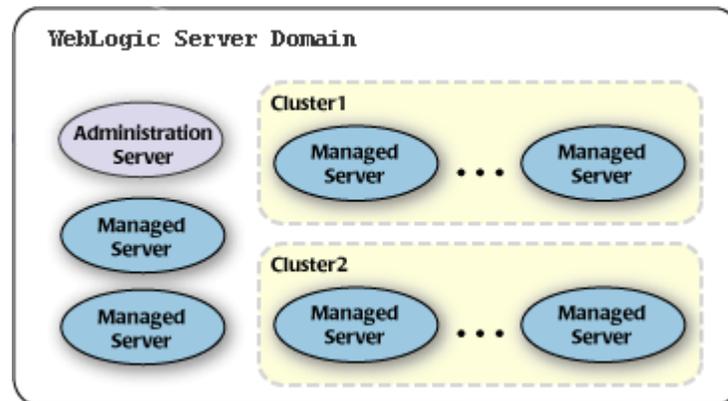
1.5 Oracle WebLogic Server Domain

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

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

Figure 1–1 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.

1.6 Directory Structure for Oracle Enterprise Content Management Suite

Figure 1–2 shows the directory structure of an Oracle Enterprise Content Management Suite installation.

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

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

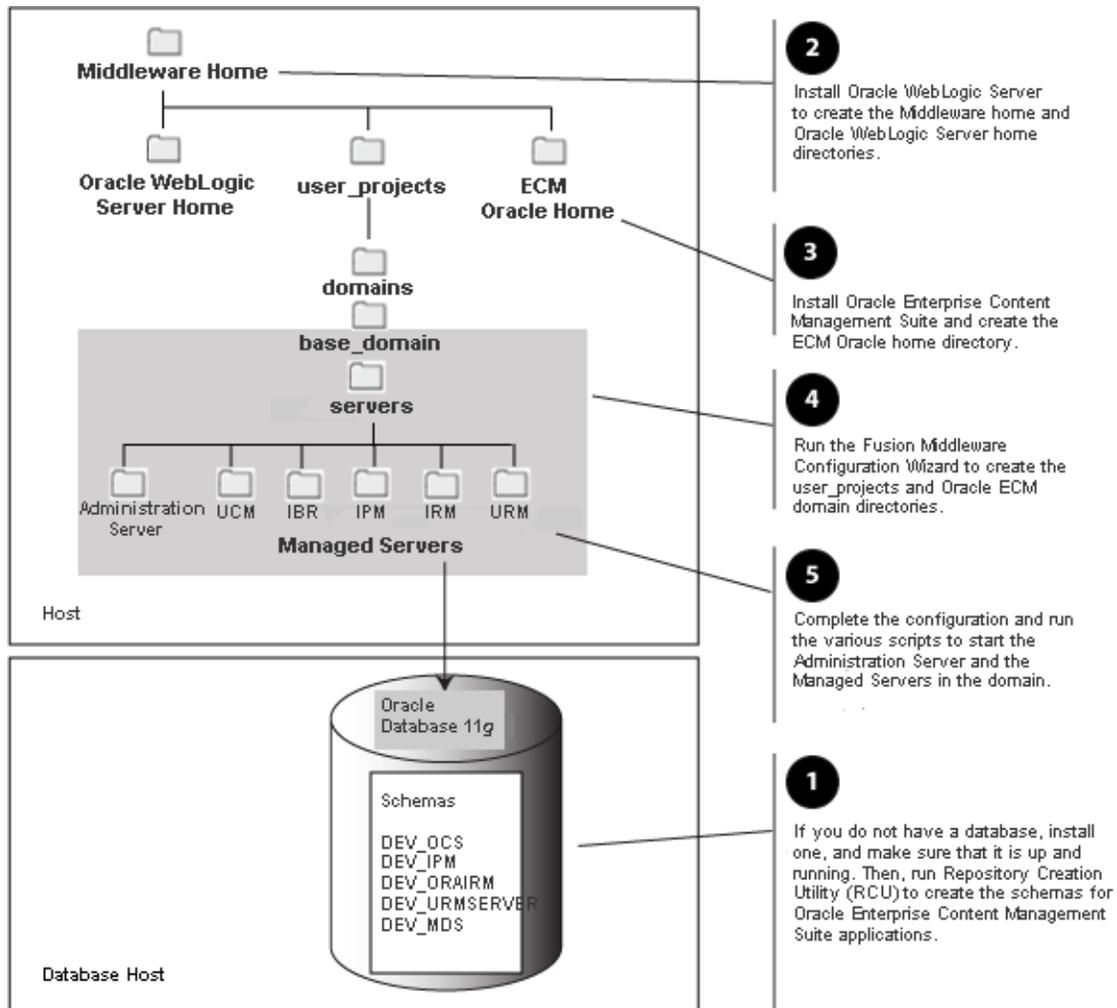
When you configure Oracle Enterprise Content Management Suite to create an Oracle WebLogic Server domain, a domain directory is created under the *MW_HOME/user_projects/domains* directory. The directory for the domain where you configure Oracle Enterprise Content Management Suite contains the Administration Server and one or more Managed Servers, each hosting an Oracle Enterprise Content

Management Suite application. Based on the application or applications that you install, the following Managed Servers are created:

- Oracle UCM Managed Server
- Oracle URM Managed Server
- Oracle IBR Managed Server
- Oracle I/PM Managed Server
- Oracle IRM Managed Server

Figure 1–2 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 1–2 Topology of an Oracle Enterprise Content Management Suite Installation



The topology in Figure 1–2 includes multiple applications configured on the same host in one Oracle WebLogic Server domain that includes only Oracle Enterprise Content Management Suite applications. The schemas for the applications are in the same database.

Creating Schemas for Oracle Enterprise Content Management Suite

This chapter explains how to use Repository Creation Utility (RCU) to create database schemas for Oracle Enterprise Content Management Suite applications, in these topics:

- [Preparing to Run Repository Creation Utility and Load Schemas](#)
- [Creating Oracle Enterprise Content Management Suite Schemas](#)

2.1 Preparing to Run Repository Creation Utility and Load Schemas

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

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

2.1.1 Database Prerequisites

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

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

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

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

2.1.2 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 Creating Oracle Enterprise Content Management Suite Schemas

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

To create Oracle Enterprise Content Management Suite schemas:

1. Insert a DVD or unzip a ZIP 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 E-Delivery at
<http://edelivery.oracle.com/>
- Oracle Fusion Middleware 11g 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 run RCU as the preceding text describes.

2. Welcome screen

Click **Next**.

3. Create Repository screen

Select **Create**.

Click **Next**.

4. Database Connection Details screen

Database Type: Select `Oracle Database`, `Microsoft SQL Server`, or `IBM DB2`.

The default is `Oracle Database`.

Before you can use SQL Server with Oracle UCM, you need to turn on snapshot isolation in the database. If you plan to use SQL Server for the back-end database for Oracle Imaging and Process Management (Oracle I/PM) 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 Oracle UCM 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 on 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 2.1.1, "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.
- 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.

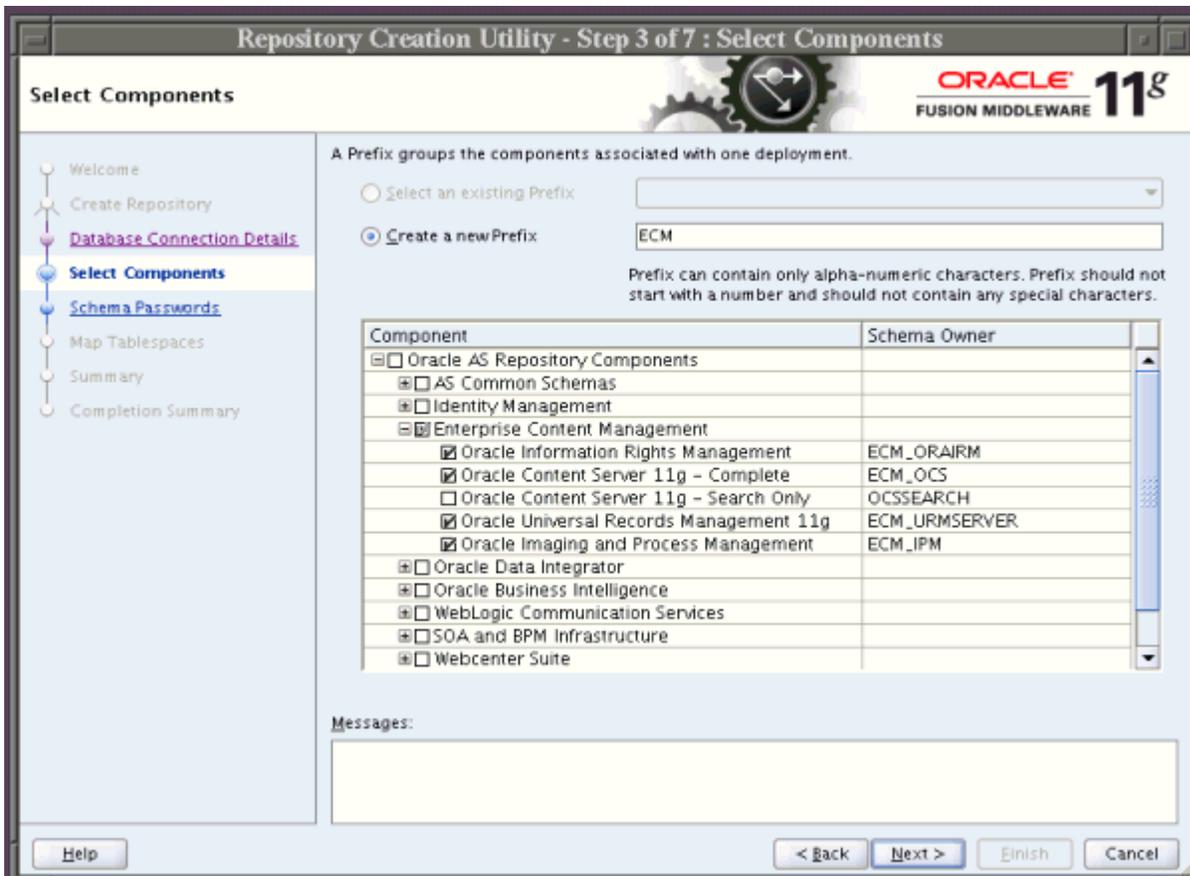
Click **Next**. The Checking Global Prerequisites dialog box appears.

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.

- Select Components screen

Figure 2–1 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 **Enterprise Content Management** in the Components list, and select one or more applications for which to create a schema:

- **Oracle Information Rights Management**
- **Oracle Content Server 11g - Complete**
- **Oracle Content Server 11g - Search Only**
- **Oracle Universal Records Management 11g**
- **Oracle Imaging and Process Management**

To create a schema for Oracle UCM, select **Oracle Content Server 11g - Complete**.

To create an OCSSEARCH schema for configuring Oracle UCM to create a search schema for Oracle Text Search or IBM DB2 database searches, select **Oracle Content Server 11g - Search Only**. For more information, see [Section 5.2.2, "Configuring the Oracle Content Server Instance."](#)

If you select **Oracle Imaging and Process Management**, you should also select **Oracle Content Server 11g - Complete** to use Oracle UCM as the Oracle I/PM repository.

Also, for Oracle WSM Policy Manager or for using Oracle I/PM 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 Oracle URM 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

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

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

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

Notes:

- For an IBM DB2 database, any tablespace that PUBLIC has access to is required to have a 32 KB page size. Oracle UCM requires a 32 KB page size to create tables at design time. All the tablespaces that PUBLIC has access to are accessible by Oracle UCM.
- 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 ECM application then would have access only to its own tablespace.

8. 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.

9. Completion Summary screen

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

Click **Close**.

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

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

Installing Oracle Enterprise Content Management Suite

This chapter explains how to install the Oracle Enterprise Content Management Suite component of Oracle Fusion Middleware, in these topics:

- [Preparing for Installation](#)
- [Installing Oracle Enterprise Content Management Suite in Oracle Fusion Middleware](#)

3.1 Preparing for Installation

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

3.1.1 Meeting System Requirements

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

- "Oracle Fusion Middleware System Requirements and Specifications" at http://www.oracle.com/technology/software/products/ias/files/fusion_requirements.htm

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

- "Oracle Fusion Middleware Supported System Configurations" at http://www.oracle.com/technology/software/products/ias/files/fusion_certification.html

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

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 Oracle I/PM Advanced Viewer.
-

3.1.2 Installing Oracle WebLogic Server in a Middleware Home

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

To install Oracle WebLogic Server in a Middleware home:

1. Insert the Oracle WebLogic Server DVD, or download the installer from the Oracle E-Delivery or Oracle Technology Network (OTN) web site.

For information about downloading Oracle WebLogic Server, see [Section 1.2, "Software Downloads for Oracle ECM 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. Either run your installer file directly from the DVD, or copy the file to your local system and run it locally, after considering these notes:
 - Before running the installer on a UNIX operating system that is 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
```

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

```
./wls1034_linux32.bin
```

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

```
wls1034_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 wls1034_generic.jar
```

```
JAVA_HOME/bin/java -d64 -jar wls1034_generic.jar
```

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

```
JAVA_HOME\bin\java -jar wls1034_generic.jar
```

3. Welcome screen

Click **Next**.

4. Choose Middleware Home Directory screen

Select **Create a new Middleware Home**.

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

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

The default Oracle Middleware home is `/Oracle/Middleware` on a UNIX operating system or `\Oracle\Middleware` on a Windows operating system. For more information, see "Middleware Home and WebLogic Home Directories" in *Oracle Fusion Middleware Installation Planning Guide*.

Click **Next**.

5. Register for Security Updates screen

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

Click **Next**.

6. Choose Install Type screen

Select **Typical** 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_3.6*
- **Windows path:** *MW_HOME\coherence_3.6*

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

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

Click **Next**.

8. Choose Shortcut Location (Windows 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 *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

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

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

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

<http://www.oracle.com/technetwork/java/javase/tech/index-jsp-136191.html>

2. Install Java Access Bridge.
3. Copy the `access-bridge.jar` and `jaccess-1_4.jar` files from your installation location to the `jre\lib\ext` directory.
4. Copy the `WindowsAccessBridge.dll`, `JavaAccessBridge.dll`, and `JAWTAccessBridge.dll` files from your installation location to the `jre\bin` directory.
5. Copy the `accessibility.properties` file to the `jre\lib` directory.

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

3.1.4 Configure a DHCP Host

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

3.1.4.1 Configuring a DHCP Host on a UNIX Operating System

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

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

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

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

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

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

3.1.4.2 Configuring a DHCP Host on a Windows Operating System

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

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

```
IP_address hostname.domainname hostname
```

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

3.1.4.3 Installing a Loopback Adapter on a Windows Operating System

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

To install a loopback adapter on a Windows operating system:

1. Open Control Panel.
2. Select **Add Hardware**.
3. In the "Welcome" window, click **Next**.

4. On the "Is the hardware connected?" window, select **Yes, I have already connected the hardware**, then click **Next**.
5. In the "The following hardware is already installed on your computer" window, in the list of installed hardware, select **Add a new hardware device**, then click **Next**.
6. In the "The wizard can help you install other hardware" window, select **Install the hardware that I manually select from a list**, then click **Next**.
7. In the "From the list of hardware types, select the type of hardware you are installing" window, select **Network adapters**, then click **Next**.
8. In the "Select Network Adapter" window, make the following selections:
 - Manufacturer: **Microsoft**
 - Network Adapter: **Microsoft Loopback Adapter**
9. Click **Next**.
10. In the "The wizard is ready to install your hardware" window, click **Next**.
11. In the "Completing the Add Hardware Wizard" window, click **Finish**.
12. Restart your computer.
13. Right-click **My Network Places** on the desktop and choose **Properties**. This displays the Network Connections control panel.
14. Right-click the connection that was just created. This is usually named **Local Area Connection 2**. Choose **Properties**.
15. On the **General** tab, select **Internet Protocol (TCP/IP)**, then click **Properties**.
16. In the Internet Protocol (TCP/IP) Properties dialog box, click **Use the following IP address**, and then do the following steps:
 - a. IP Address: Enter a nonroutable IP for the loopback adapter, such as one of the following nonroutable addresses:
 - 192.168.x.x (x is any value between 1 and 255)
 - 10.10.10.10
 - b. Subnet mask: Enter 255.255.255.0.
 - c. Record the values you entered. You will need them later in this procedure.
 - d. Leave all other fields empty.
 - e. Click **OK**.
17. In the Local Area Connection 2 Properties dialog box, click **OK**.
18. Close the Network Connections control panel.
19. Restart your computer.

3.1.4.4 Removing a Loopback Adapter from a Windows Operating System

You can remove a loopback adapter through Control Panel.

To remove a loopback adapter from a Windows operating system:

1. Start the System control panel.
Select **Start > Control Panel > System**.
2. On the **Hardware** tab, click **Device Manager**.

3. In the Device Manager window, expand **Network adapters**. You should see **Microsoft Loopback Adapter**.
4. Right-click **Microsoft Loopback Adapter** and select **Uninstall**.
5. Click **OK**.

3.1.5 Installing on a Non-Networked Computer

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

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

3.1.6 Installing on a Multihomed Computer

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

The installer picks up the fully qualified domain name from the first entry in the `hosts` file:

- **UNIX path:** `/etc/hosts`
- **Windows path:** `%SYSTEMROOT%\system32\drivers\etc\hosts`

For example, the installer would pick up `myhost1.example.com` for configuration if your file contains the following entries:

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

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

3.2 Installing Oracle Enterprise Content Management Suite in Oracle Fusion Middleware

You can install Oracle Enterprise Content Management Suite before or after you create schemas for the suite's applications. When you install Oracle Enterprise Content Management Suite, you perform a base installation of the following products in an ECM Oracle home directory on your system:

- Oracle Universal Content Management (Oracle UCM)
- Oracle Inbound Refinery (Oracle IBR)
- Oracle Imaging and Process Management (Oracle I/PM)
- Oracle Information Rights Management (Oracle IRM)
- Oracle Universal Records Management (Oracle URM)

You can install Oracle Enterprise Content Management Suite before or after you create schemas for the suite's applications. After installation, you can deploy any of these products to an Oracle WebLogic Server domain, as applications, by creating or extending an Oracle WebLogic Server domain.

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

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

<http://www.sunfreeware.com>

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

3.2.1 Creating a Symbolic Link to the `chmod` Command on a Solaris System

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

To create a symbolic link to the `chmod` command:

1. Log in as the `root` user.
2. Execute the following command as `root`:

```
ln -s /usr/bin/chmod /usr/local/bin/chmod
```
3. Log out, and then log back in with a different user name to start the installation.
Running the installer as the `root` user is not supported.

3.2.2 Locating Installation Log Files

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

- **UNIX location:** `USER_HOME/oraInventory/logs/installdate_time`
- **Windows location:** `USER_HOME\oraInventory\logs\installdate_time`

3.2.3 Starting the Installer

You can start the Oracle Enterprise Content Management Suite installer from Disk 1 of the suite's media:

- **UNIX command:**

```
ecm_media_loc/Disk1/runInstaller -jreLoc jre_location
```

If you do not specify the JRE location, you will be prompted for it.

- **Windows command:**

```
ecm_installer_loc/Disk1/setup.exe -jreLoc jre_location
```

If you double-click `setup.exe`, you will be prompted for the JRE location. After you enter the path, click **Enter** to start the Oracle ECM installation.

The installer requires the location of a Java Runtime Environment (JRE) on your system. A JRE was installed with Oracle Fusion Middleware. [Table 3-1](#) shows the default JRE locations.

Table 3–1 Default JRE Locations

Operating System	Production Environment	Development Environment
UNIX	<i>MW_HOME/jrockit_160_20_string/jre</i>	<i>MW_HOME/jdk160_21/jre</i>
Windows	<i>MW_HOME\jrockit_160_20_string\jre</i>	<i>MW_HOME\jdk160_21\jre</i>

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

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

3.2.4 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**.

3.2.5 Installing Oracle Enterprise Content Management Suite

After you have started the installer, as described in [Section 3.2.3](#), follow the instructions in [Table 3–2](#) to install Oracle Enterprise Content Management Suites.

If you need additional help with any of the installation screens, see [Appendix A](#), "Oracle Enterprise Content Management Suite Installation Screens," or click **Help** to access the online help.

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

Table 3–2 Installation Procedure for Oracle Enterprise Content Management Suite

Step	Screen	Actions
1	Welcome	Click Next to begin the installation process.
2	Install Software Updates	<p>Specify any software updates to install before you install Oracle Enterprise Content Management Suite.</p> <p>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.</p> <p>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.</p> <p>If you do not want to update any software, select Skip Software Updates, and then click Next to continue the installation.</p>
3	Prerequisite Checks	<p>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.</p> <p>If you want to stop the installation process while you fix a prerequisite error, click Abort.</p> <p>If you want to continue the installation without fixing an error, click Continue.</p> <p>Click Next to continue the installation after the prerequisite checks complete with no errors.</p>
4	Specify Installation Location	<p>Specify the Middleware home (<i>MW_HOME</i>) and ECM Oracle home (<i>ECM_ORACLE_HOME</i>) locations.</p> <p>Enter values into the following fields:</p> <ul style="list-style-type: none"> ■ Oracle Middleware Home: Select the Middleware home directory, which was created during the installation of Oracle WebLogic Server. The default Oracle Middleware home is <code>/Oracle/Middleware</code> on a UNIX operating system or <code>\Oracle\Middleware</code> on a Windows operating system. ■ Oracle Home Directory: Specify the directory where you want to install Oracle Enterprise Content Management Suite. If you specify a directory that already exists, it must be empty and inside the Middleware home directory. If you specify a new directory, the installer creates it inside the Middleware home directory. <p>The installation directory becomes the ECM Oracle home directory for Oracle Enterprise Content Management Suite. Run-time components cannot write to this directory. The default ECM Oracle home is <code>MW_HOME/Oracle_ECM1</code> on a UNIX operating system or <code>MW_HOME\Oracle_ECM1</code> on a Windows operating system.</p> <p>Note: This document refers to this directory as the ECM Oracle home to avoid confusion with the Oracle home directories of other Java components of Oracle Fusion Middleware. For more information, see "Oracle Home and Oracle Common Home Directories" in <i>Oracle Fusion Middleware Installation Planning Guide</i>.</p> <p>Click Next to continue.</p>

Table 3–2 (Cont.) Installation Procedure for Oracle Enterprise Content Management

Step	Screen	Actions
5	Installation Summary	<p>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.</p> <p>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.</p> <p>Click Install to start the software installation.</p>
6	Installation Progress	<p>Monitor the progress of your installation.</p> <p>If the installer prompts you to go to <code>Disk 2</code>, specify the location of <code>Disk 2</code>, and click OK to resume the installation.</p> <p>If you want to stop the installation, click Cancel.</p> <p>After the progress reaches 100%, click Next to go to the last screen.</p>
7	Installation Completed	<p>Click Save to save the installation configuration, and then click Finish to exit the installer.</p>

Configuring Oracle Enterprise Content Management Suite

This chapter explains how to configure an Oracle WebLogic Server domain for Oracle Enterprise Content Management Suite applications, in these topics:

- [Preparing to Configure Oracle Enterprise Content Management Suite](#)
- [Creating an Oracle WebLogic Server Domain](#)
- [Extending an Existing Domain](#)
- [Extending a Domain in an SSL Environment](#)
- [Increasing the Java VM Heap Size for Managed Servers](#)
- [Setting Up Fonts on a UNIX System](#)
- [Installing Libraries and Setting Environment Variables for Outside In Technology](#)
- [Configuring SSL for Oracle ECM Applications](#)
- [Reassociating the Identity Store with an External LDAP Authentication Provider](#)
- [Adding Users to Oracle Internet Directory](#)
- [Installing Fonts for National Language Support on a UNIX System](#)
- [Configuring Single Sign-On \(SSO\)](#)
- [Configuring Managed Server Clusters](#)
- [Setting Up Oracle Web Services Manager Security](#)

4.1 Preparing to Configure Oracle Enterprise Content Management Suite

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

- Oracle Universal Content Management (Oracle UCM)
- Oracle Inbound Refinery (Oracle IBR)
- Oracle Imaging and Process Management (Oracle I/PM)
- Oracle Information Rights Management (Oracle IRM)
- Oracle Universal Records Management (Oracle URM)

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.

Important: Each of these applications needs to run in its own Managed Server or its own cluster of Managed Servers. You cannot deploy Oracle UCM, Oracle IBR, Oracle I/PM, Oracle IRM, or Oracle URM to a Managed Server or cluster that already has another application deployed. Oracle ECM applications should not be deployed to the Administration Server.

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: Oracle Enterprise Content Management Suite 11g does not support running Oracle UCM, Oracle IBR, or Oracle URM as a service on a Windows operating system.

For Oracle I/PM 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 *Oracle Fusion Middleware Administrator's Guide for Oracle Imaging and Process Management*.

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

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

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

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

Note: You cannot extend a domain that has an Oracle ECM 11.1.1.2.1 or 11.1.1.3.0 application to include an Oracle ECM 11.1.1.4.0 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, "Oracle Enterprise Content Management Suite Configuration Screens,"](#) or click **Help** on the screen in the installer to access the online help.

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

4.2 Creating an Oracle WebLogic Server Domain

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

The configuration wizard is in the following directory. *ECM_ORACLE_HOME* represents the ECM Oracle home directory, where Oracle Enterprise Content Management Suite is installed:

- **UNIX path:** *ECM_ORACLE_HOME*/common/bin
- **Windows path:** *ECM_ORACLE_HOME*\common\bin

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

- **UNIX script:**
ECM_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:**
ECM_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 4–1](#) describes the steps for creating a domain and provides links to descriptions of the screens in [Appendix B, "Oracle Enterprise Content Management Suite Configuration Screens."](#)

Table 4–1 Procedure for Creating a New Domain

Step	Screen	When This Screen Appears	Description and Action Required
1	None.	Always	<p>Start Fusion Middleware Configuration Wizard:</p> <ul style="list-style-type: none"> ■ UNIX script: <code>ECM_ORACLE_HOME/common/bin/config.sh</code> <code>[-log=log_file_name]</code> ■ Windows script: <code>ECM_ORACLE_HOME\common\bin\config.cmd</code> <code>[-log=log_file_name]</code>
2	Welcome	Always	<p>Select Create a new WebLogic Domain. Click Next to continue.</p>
3	Select Domain Source	Always	<p>Select Generate a domain configured automatically to support the following products, and then select one or more of these products:</p> <ul style="list-style-type: none"> ■ Oracle Universal Records Management Server ■ Oracle Information Rights Management ■ Oracle Universal Content Management - Inbound Refinery ■ Oracle Universal Content Management - Content Server ■ Oracle Imaging and Process Management <p>When you select Oracle Imaging and Process Management, you also need to select Oracle Universal Content Management - Content Server.</p> <p>When you select any Oracle ECM 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 ECM application will also be deselected.</p> <p>If you want a remote deployment of a Site Studio for External Applications web site, you can select Oracle Universal Content Management - SSXA Server to create an Oracle WebLogic Server domain with a Managed Server that has the files required to run the web site.</p> <p>To create a domain that includes Oracle Web Services Manager (Oracle WSM) Policy Manager, select Oracle WSM Policy Manager.</p> <p>Click Next to continue.</p>

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

Step	Screen	When This Screen Appears	Description and Action Required
4	Specify Domain Name and Location	Always	<p>Enter the name of the domain you want to create in the Domain name field.</p> <p>The default location for the domain follows (<i>MW_HOME</i> represents the Middleware home directory):</p> <ul style="list-style-type: none"> ▪ UNIX path: <i>MW_HOME</i>/user_projects/domains ▪ Windows path: <i>MW_HOME</i>\user_projects\domains <p>You can specify a different location in the Domain location field.</p> <p>Note: Record the domain name and location from this screen because you will need them later to start the Administration Server.</p> <p>You can specify the location of the Oracle Enterprise Content Management Suite application in the Application location field. The default location is <i>MW_HOME</i>/user_projects/applications/.</p> <p>Click Next to continue.</p>
5	Configure Administrator User Name and Password	Always	<p>The User name field has the default administrator user name, <code>weblogic</code>. You can specify a different administrator user name.</p> <p>In the User password field, enter the password for the administrator user.</p> <p>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.</p> <p>Click Next to continue.</p>
6	Configure Server Start Mode and JDK	Always	<p>Under WebLogic Domain Startup Mode, Development Mode is the default mode. For a production system, select Production Mode.</p> <p>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_21, and the default JDK for production mode is JRockit SDK 1.6.0_20, 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.</p> <p>Click Next to continue.</p>

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

Step	Screen	When This Screen Appears	Description and Action Required
7	Configure JDBC Component Schema	Always	<p>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:</p> <ul style="list-style-type: none"> ■ 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. <p>Specify the database that contains the application schema or schemas.</p> <p>For Oracle RAC databases, specify the service name of one of the nodes in this field. For example: sales.example.com.</p> <ul style="list-style-type: none"> ■ 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. <p>Click Next to continue.</p>
8	Test Component Schema	Always	<p>The configuration wizard automatically tests the connection to the JDBC component schema.</p> <p>If the test fails, click Previous to correct the component schema information, and then click Next to retest the connection.</p> <p>After the test succeeds, click Next to continue.</p>

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

Step	Screen	When This Screen Appears	Description and Action Required
9	Select Optional Configuration	Always	<p>Optionally, select any or all of these options for configuring the Administration Server and Managed Servers:</p> <ul style="list-style-type: none"> ■ JMS Distributed Destination ■ Administration Server ■ Managed Servers, Clusters and Machines ■ Deployments and Services ■ RDBMS Security Store <p>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.</p> <p>For Oracle IRM, you should select Administration Server, Managed Servers, Clusters and Machines, and Deployments and Services.</p> <p>Note: To use clusters, you need a license for Oracle WebLogic Server Enterprise Edition.</p> <p>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.</p>
10	Configure the Administration Server	If you selected Administration Server on the Select Optional Configuration screen	<p>The default listen port number for the Administration Server is 7001, which you can change.</p> <p>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.</p> <p>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 <code>wlst.sh</code> file or set them in the <code>CONFIG_JVM_ARGS</code> environment variable:</p> <pre>-Dweblogic.security.SSL.ignoreHostnameVerification=true -Dweblogic.security.TrustKeyStore=KeyStoreName</pre> <p><i>KeyStoreName</i> is the name of the keystore in use (DemoTrust for the built-in demonstration certificate). The <code>wlst.sh</code> file is in the <code>bin</code> subdirectory of the <code>common</code> directory in the ECM Oracle home directory.</p> <p>Click Next to continue.</p>

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

Step	Screen	When This Screen Appears	Description and Action Required
11	Configure Managed Servers	If you selected Managed Servers, Clusters and Machines on the Select Optional Configuration screen.	<p>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.</p> <p>Table 4–2 lists the default port values for the Managed Servers that run Oracle Enterprise Content Management Suite applications.</p> <p>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.</p> <p>For Oracle IRM, SSL is enabled by default, with port number 16101. SSL needs to be configured so that Oracle IRM Desktop does not show prompts to accept certificates when it contacts the Managed Server. The certificate used must be trusted by Microsoft Internet Explorer on computers running Oracle IRM Desktop.</p> <p>Click Next to continue.</p>
12	Configure Clusters	If you selected Managed Servers, Clusters and Machines on the Select Optional Configuration screen.	<p>Optionally, configure one or more clusters.</p> <p>Notes:</p> <ul style="list-style-type: none"> ■ 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. <p>Click Next to continue.</p>
13	Assign Servers to Clusters	If you configured any clusters on the Configure Clusters screen	<p>Assign two or more of the Managed Servers in the domain to each cluster.</p> <p>Click Next to continue.</p>
14	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	<p>Create a proxy application for each Managed Server that you did not assign to a cluster in the domain.</p> <p>Click Next to continue.</p>
15	Configure Machines	If you selected Managed Servers, Clusters and Machines on the Select Optional Configuration screen.	<p>Optionally, configure machines to host Managed Servers, and assign a Managed Server to each machine.</p> <p>Click Next to continue.</p>
16	Assign Servers to Machines	If you added any machines on the Configure Machines screen	<p>Assign at least one server to each machine.</p> <p>Click Next to continue.</p>

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

Step	Screen	When This Screen Appears	Description and Action Required
17	Target Deployments to Clusters or Servers	If you selected Deployments and Services on the Select Optional Configuration screen.	<p>Optionally, assign each application to the Administration Server, a Managed Server, or a cluster of Managed Servers.</p> <p>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 <code>persistent-store-type</code> as <code>replicated_if_clustered</code>. If the Oracle IRM web application is deployed on a clustered server, the in-effect <code>persistent-store-type</code> will be replicated. Otherwise, memory is the default.</p> <p>When deploying Oracle IRM to a cluster, make sure that the Oracle IRM application is deployed to all nodes.</p> <p>Click Next to continue.</p>
18	Target Services to Clusters or Servers	If you selected Deployments and Services on the Select Optional Configuration screen.	<p>Optionally, modify how your services are targeted to servers or clusters.</p> <p>Click Next to continue.</p>
19	Configure RDBMS Security Store Database	If you selected RDBMS Security Store on the Select Optional Configuration screen.	<p>Optionally, make changes to your RDBMS security store.</p> <p>Click Next to continue.</p>
20	Configuration Summary	Always	<p>Review your configuration and make any corrections or updates by following the instructions on the screen.</p> <p>You can click Previous on each screen to go back to a screen where you want to change the configuration.</p> <p>When the configuration is satisfactory, click Create to create the domain.</p>
21	Creating Domain	Always	<p>On a Windows operating system, you can select Start Admin Server to start the Administration Server as soon as the configuration is done.</p> <p>When the domain is created successfully, click Done.</p>

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

Table 4–2 Default Ports for Managed Servers

Managed Server	Default Listen Port	Default SSL Port	Port Range
Oracle I/PM	16000	16001	16000–16099
Oracle IRM	16100	16101	16100–16199
Oracle UCM	16200	16201	16200–16299
Oracle IBR	16250	16251	16200–16299
Oracle URM	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 10.2, "Starting Managed Servers."](#)

4.3 Extending an Existing Domain

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

- **UNIX path:** *ECM_ORACLE_HOME/common/bin*
- **Windows path:** *ECM_ORACLE_HOME\common\bin*

Note: You cannot extend a domain that has an Oracle ECM 11.1.1.2.1 or 11.1.1.3.0 application to include an Oracle ECM 11.1.1.4.0 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 an Oracle IRM Managed Server. Or you could extend an Oracle I/PM domain to include Oracle SOA Suite.

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

```
<include name="soa-ibm-addon.jar"/>
```

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

Table 4–3 Procedure for Extending an Existing Domain

Step	Screen	When This Screen Appears	Description and Action Required
1	None.	Always	<p>Start Fusion Middleware Configuration Wizard:</p> <ul style="list-style-type: none"> ■ UNIX script: <code>ECM_ORACLE_HOME/common/bin/config.sh [-log=log_file_name]</code> ■ Windows script: <code>ECM_ORACLE_HOME\common\bin\config.cmd [-log=log_file_name]</code>
2	Welcome	Always	<p>Select Extend an existing WebLogic Domain.</p> <p>Click Next to continue.</p>
3	Select a WebLogic Domain Directory	Always	<p>Select a directory for adding your applications or services, or both.</p> <p>Click Next to continue.</p>
4	Select Extension Source	Always	<p>Select Extend my domain automatically to support the following added products, and then select one or more of these products:</p> <ul style="list-style-type: none"> ■ Oracle Universal Records Management Server ■ Oracle Information Rights Management ■ Oracle Universal Content Management - Inbound Refinery ■ Oracle Universal Content Management - Content Server ■ Oracle Imaging and Process Management <p>When you select Oracle Imaging and Process Management, you also need to select Oracle Universal Content Management - Content Server, if Oracle UCM is not already configured.</p> <p>When you select any Oracle ECM 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 ECM application will also be deselected.</p> <p>If you want a remote deployment of a Site Studio for External Applications web site, you can select Oracle Universal Content Management - SSXA Server to extend an Oracle WebLogic Server domain with a Managed Server that has the files required to run the web site.</p> <p>To extend a domain that includes Oracle Web Services Manager (Oracle WSM) Policy Manager, select Oracle WSM Policy Manager.</p> <p>Click Next to continue.</p>

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

Step	Screen	When This Screen Appears	Description and Action Required
5	Configure JDBC Component Schema	Always	<p>Configure each component schema, including the Oracle WSM MDS schema if it was created with Repository Creation Utility (RCU), in the following fields:</p> <ul style="list-style-type: none"> ■ Component Schema: Select a component schema row. ■ Vendor: Select a database vendor from the list. ■ Driver: Leave the default driver for the database vendor selected, or select a driver for the component schema from the list. ■ Schema Owner: Enter the user name of the application schema owner, specified during schema creation with Repository Creation Utility (RCU). ■ Schema Password: Enter the schema password, specified during schema creation with RCU. ■ DBMS/Service: Enter the name of the database instance if Oracle's Driver (Thin) for Instance connections is selected in the Driver field, or enter the service name (global database name) if Oracle's Driver (Thin) for Service connections is selected in the Driver field. For Microsoft SQL Server, you must enter a database name because there is no service name. <p>Specify the database that contains the application schema or schemas.</p> <p>For Oracle RAC databases, specify the service name of one of the nodes in this field. For example: sales.example.com.</p> <ul style="list-style-type: none"> ■ Host Name: Specify the name of the machine on which your database resides, in the format <code>host.example.com</code>. 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. <p>Click Next to continue.</p>
6	Test Component Schema	Always	<p>The configuration wizard automatically tests the connection to the JDBC component schema.</p> <p>If the test fails, click Previous to correct the component schema information, and then click Next to retest the connection.</p> <p>After the test succeeds, click Next to continue.</p>

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

Step	Screen	When This Screen Appears	Description and Action Required
7	Select Optional Configuration	Always	<p>Optionally, select any or all of these options for configuring Managed Servers:</p> <ul style="list-style-type: none"> ■ JMS Distributed Destination ■ Managed Servers, Clusters and Machines ■ Deployments and Services ■ RDBMS Security Store <p>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.</p> <p>Note: To use clusters, you need a license for Oracle WebLogic Server Enterprise Edition.</p> <p>For Oracle IRM, you should select Administration Server, Managed Servers, Clusters and Machines, and Deployments and Services.</p> <p>If you are extending a domain that already includes Oracle UCM with Oracle I/PM and plan to use Oracle UCM 11g as the Oracle I/PM repository, select Managed Servers, Clusters and Machines so you can configure a separate machine for running the Oracle I/PM Managed Server.</p> <p>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.</p>
8	Configure Managed Servers	If you selected Managed Servers, Clusters and Machines on the Select Optional Configuration screen.	<p>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.</p> <p>Table 4–2 lists the default port values for the Managed Servers that run Oracle Enterprise Content Management Suite applications.</p> <p>To change the SSL configuration for a Managed Server, you can select SSL enabled and set or change the SSL listen port value.</p> <p>For Oracle IRM, SSL is enabled by default, with port number 16101. SSL needs to be configured so that Oracle IRM Desktop does not show prompts to accept certificates when it contacts the Managed Server. The certificate used must be trusted by Microsoft Internet Explorer on computers running Oracle IRM Desktop.</p> <p>Click Next to continue.</p>
9	Configure Clusters	If you selected Managed Servers, Clusters and Machines on the Select Optional Configuration screen.	<p>Optionally, change the cluster configuration.</p> <p>Notes:</p> <ul style="list-style-type: none"> ■ 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. <p>Click Next to continue.</p>

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

Step	Screen	When This Screen Appears	Description and Action Required
10	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.
11	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.
12	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 Oracle UCM with Oracle I/PM and plan to use Oracle UCM 11g as the Oracle I/PM repository, configure a separate machine and assign the Oracle I/PM Managed Server to it. Click Next to continue.
13	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.
14	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 <code>persistent-store-type</code> as <code>replicated_if_clustered</code> . If the Oracle IRM web application is deployed on a clustered server, the in-effect <code>persistent-store-type</code> will be replicated. Otherwise, memory is the default. Make sure that the Oracle IRM application is not deployed to one of the servers in a cluster. Click Next to continue.
15	Target Services to Clusters or Servers	If you selected Deployments and Services on the Select Optional Configuration.	Optionally, modify how your services are targeted to servers or clusters. Click Next to continue.
16	Configuration Summary	Always.	When the configuration is satisfactory, click Extend to extend the domain.
17	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 10.2, "Starting Managed Servers."](#)

4.4 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 4-3](#).

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=DemoTrustKeyStorePassPhrase`
 - `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.

4.5 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) for the JRockit JDK or to 512 MB for the Sun JDK. 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 the permanent generation, 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 10.4, "Starting Node Manager."](#)
- [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 10.2, "Starting Managed Servers."](#)

4.5.1 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 4–4](#) shows parameters to specify for Sun and JRockit Java VMs on UNIX and Windows operating systems. Other Java VMs may have different values.

Table 4–4 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 10.3, "Restarting a Managed Server."](#)

4.5.2 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 4-4 shows parameters to specify for Sun and JRockit Java VMs on UNIX and Windows operating systems. Other Java VMs may have different values.

4.6 Setting Up Fonts on a UNIX System

On a UNIX operating system, you need to make sure TrueType fonts are set up for Oracle I/PM, Oracle IBR, and Oracle UCM Dynamic Converter. If you are using a language other than English, you also need to set up fonts for national language support.

4.6.1 Setting Up TrueType Fonts on a UNIX System

For Oracle I/PM, Oracle IBR, and Oracle UCM Dynamic Converter to work correctly on a UNIX operating system, you need to set up TrueType fonts on the machine where Oracle I/PM, Oracle IBR, or the Dynamic Converter is running. If these fonts are not available on your system, you need to install them. Then you can configure Oracle IBR with the path to the font directory, as follows. For information about configuring the path to the font directory for Oracle I/PM once the fonts are installed, see [Section 7.1.4, "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, Oracle I/PM requires the GNU Compiler Collection (GCC) package 3.4.2 or later in the /usr/local/packages directory.

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

<http://www.sunfreeware.com>

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

- AIX: /usr/lpp/X11/lib/X11/fonts/TrueType
- HP-UX Itanium: /usr/lib/X11/fonts/TrueType

To set the path to the font directory in Oracle IBR:

1. Log in to Oracle IBR.
2. Select **Conversion Settings**, then **Third-Party Application Settings**, and then **General OutsideIn Filter Options**.
3. Click **Options**.
4. Enter the path to the TrueType fonts in the **Path to fonts** field.

For example:

```
/usr/share/x11/fonts/FTP
```

5. Click **Update**.

4.6.2 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.

4.7 Installing Libraries and Setting Environment Variables for Outside In Technology

Oracle UCM, Oracle IBR, Oracle I/PM, and the Oracle I/PM Advanced Viewer for clients use Outside In Technology (OIT), which requires certain libraries that are not part of Oracle ECM. Before an Oracle UCM, Oracle IBR, or Oracle I/PM 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.

4.7.1 Installing Libraries for Outside In Technology on UNIX Platforms

Before you start an Oracle UCM, Oracle IBR, or Oracle I/PM 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 from the following web site:

<http://hpacxx.external.hp.com/gcc>

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 Oracle I/PM or Oracle UCM 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.

4.7.2 Setting Library Paths in Environment Variables on UNIX Platforms

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

- Environment variables for library paths for Oracle I/PM
 - Solaris Sparc:


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

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
```
- Environment variables for library paths for Oracle UCM with Dynamic Converter and Oracle IBR
 - Solaris Sparc:


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

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

Add the following line to the Oracle IBR `intradoc.cfg` file at `DomainHome/ucm/ibr/bin`:

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

Then restart Oracle IBR, as described in [Section 10.3, "Restarting a Managed Server."](#)
 - 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 Oracle UCM 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 Oracle I/PM, the Oracle IBR Managed Server, or the Oracle UCM Dynamic Converter.

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

OutsideIn 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:

- `vc_redist_x86.exe`
- `vc_redist_x64.exe`
- `vc_redist_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.

4.8 Configuring SSL for Oracle ECM Applications

You can configure SSL for Oracle ECM applications running in a production environment 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 ECM Oracle home directory.

4.8.1 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 Oracle IRM Desktop and the Oracle IRM server application must be over SSL because sensitive information such as passwords are communicated.

Other uses of SSL, such as between OHS and Managed Servers, the Administration Server, and the LDAP authentication provider are optional.

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

4.8.2 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.

4.8.2.1 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 where Oracle IRM 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 Oracle IRM server, which is the name that Oracle IRM will use 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 for Oracle IRM and a Self-Signed Root Certificate.

3. Run the `ImportPrivateKey` utility to package the Private Key and Self-Signed Root Certificate into a 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 3.1.2, "Installing Oracle WebLogic Server in a Middleware Home."](#)

- **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.

4.8.2.2 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.

4.9 Reassociating the Identity Store with an External LDAP Authentication Provider

In a production system, Oracle Enterprise Content Management Suite applications need to use an external Lightweight Directory Application Protocol (LDAP) authentication provider rather than the Oracle WebLogic Server embedded LDAP server, which is part of the default configuration. You need to reassociate the identity store for your application with one of the following external LDAP authentication providers before you complete the configuration of a Managed Server, 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 Oracle I/PM application, the user who logs in first to an Oracle I/PM Managed Server is provisioned with full security throughout the server. It is easier to reassociate the identity store for Oracle I/PM with an external LDAP authentication provider before the first user logs in, completes the configuration of the Oracle I/PM Managed Server, and connects it to the Oracle Universal Content Management (Oracle UCM) repository.

For an Oracle IRM application, the Oracle IRM domain, which is different from the Oracle WebLogic Server domain, gets created the first time a user logs in to the Oracle IRM Management Console. The first user who logs in to the console is made the Domain Administrator for the Oracle IRM instance. Before you migrate user data for Oracle IRM, the users need to be in the target LDAP identity store. 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.

4.9.1 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 4-5](#) lists the available authenticator types.

Table 4–5 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 an 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. Oracle IRM uses the export folder path to decide where to write out the user and group details, so the 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 ECM_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 ECM 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 `batchXXX`, 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:

```
setIRMEExportFolder('')
```

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 10.1, "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 4–5](#).
- 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.

1. 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 10.2, "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 10.3, "Restarting a Managed Server."](#)
13. For an 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 ECM_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 an Oracle IRM role of Domain Administrator, then, after migration, the user in Oracle Internet Directory with the user name `weblogic` would have the Oracle IRM role of Domain Administrator.

4.9.2 Refreshing GUID Values in Oracle I/PM Security Tables

If you change the LDAP providers, the global user IDs (GUIDs) in the Oracle I/PM security tables will be invalid. Oracle I/PM 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 Oracle I/PM security tables with WLST commands or with Fusion Middleware Control.

Only users and groups that exist in both LDAP providers will have GUIDs refreshed. Oracle I/PM 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 Oracle I/PM database.

4.9.2.1 Refreshing GUID values in Oracle I/PM 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 Oracle I/PM security tables with WLST:

1. Log in to Oracle WebLogic Server Administration Server.
2. Navigate to the Oracle ECM home directory: `MW_HOME/ECM_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 IPM 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 Oracle I/PM to verify user and group security.

4.9.2.2 Refreshing GUID values in Oracle I/PM 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 Oracle I/PM 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 ECM domain folder, then **IPM_Cluster**, and then the name of the Oracle I/PM 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 Oracle I/PM to verify user and group security.

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

To add users to Oracle Internet Directory:

1. Invoke Oracle Directory Services Manager and connect to the Oracle Internet Directory server.
2. From the task selection bar, select **Data Browser**.
3. On the toolbar, select the **Create a new entry** icon. Alternatively, right-click any entry and choose **Create**.

The Create New Entry wizard starts.

4. Specify the object classes for the new entry.

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

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

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

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

6. Click **Next**.

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

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

8. Click **Next**.

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

9. Click **Finish**.

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

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

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

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

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

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

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

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

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

4.11 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.

4.12 Configuring Single Sign-On (SSO)

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

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

[Table 4–6](#) shows which SSO solutions you can use with which Oracle ECM applications. The sections that follow provide references to information about using SSO with these applications.

Table 4–6 Single Sign-On Solutions for Oracle ECM Applications

Application	Oracle Access Manager 11g	Oracle Access Manager 10g	OSSO	WNA
Oracle UCM Content Server	Supported	Supported	Supported	Supported
Oracle I/PM	Supported	Supported	Supported	Supported
Oracle IRM Web Interface	Supported	Not supported	Supported	Supported
Oracle IRM Desktop	Not supported	Supported (limited)	Not supported	Supported
Oracle URM	Supported	Supported	Supported	Supported

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

4.12.1 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 8.4, "Integrating Oracle IRM with Oracle Access Manager 11g."](#) For information about configuring it for Oracle I/PM, see *Oracle Fusion Middleware Administrator's Guide for Oracle Imaging and Process Management*. For information about configuring it for Oracle UCM, Oracle IBR, or Oracle URM, see "Configuring Oracle UCM for Single Sign-On" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Content Server*.

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

[Table 4–7](#) shows where to get more information about configuring Oracle Access Manager 11g for Oracle ECM applications.

Table 4–7 Oracle Access Manager 11g Configuration for Oracle ECM Applications

Application	Configuration Information
Oracle UCM Content Server	"Configuring Oracle Access Manager 11g with Oracle UCM" in <i>Oracle Fusion Middleware System Administrator's Guide for Oracle Content Server</i>
Oracle I/PM	"Integrating Oracle Access Manager 11g With Oracle I/PM" in <i>Oracle Fusion Middleware Administrator's Guide for Oracle Imaging and Process Management</i>
Oracle IRM Web Interface	Section 8.4, "Integrating Oracle IRM with Oracle Access Manager 11g"
Oracle IRM Desktop	Not supported
Oracle URM	"Configuring Oracle Access Manager 11g with Oracle UCM" in <i>Oracle Fusion Middleware System Administrator's Guide for Oracle Content Server</i>

[Table 4–8](#) shows where to get more information about configuring Oracle Access Manager 10g for Oracle ECM applications.

Table 4–8 Oracle Access Manager 10g Configuration for Oracle ECM Applications

Application	Configuration Information
Oracle UCM Content Server	"Configuring Oracle Access Manager 10g with Oracle UCM" in <i>Oracle Fusion Middleware System Administrator's Guide for Oracle Content Server</i>
Oracle I/PM	"Integrating Oracle Access Manager 10g With Oracle I/PM" in <i>Oracle Fusion Middleware Administrator's Guide for Oracle Imaging and Process Management</i>
Oracle IRM Web Interface	Not supported
Oracle IRM Desktop	Section 8.4, "Integrating Oracle IRM with Oracle Access Manager 11g"
Oracle URM	"Configuring Oracle Access Manager 11g with Oracle UCM" in <i>Oracle Fusion Middleware System Administrator's Guide for Oracle Content Server</i>

4.12.2 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 *Oracle Fusion Middleware Application Security Guide*.

[Table 4–9](#) shows where to get more information about configuring OSSO for Oracle ECM applications.

Table 4–9 OSSO Configuration for Oracle ECM Applications

Application	Configuration Information
Oracle UCM Content Server	"Configuring Oracle Single Sign-On for Oracle UCM" in <i>Oracle Fusion Middleware System Administrator's Guide for Oracle Content Server</i>
Oracle I/PM	"Configuring Oracle Single Sign-On for Oracle I/PM" in <i>Oracle Fusion Middleware Administrator's Guide for Oracle Imaging and Process Management</i>
Oracle IRM Web Interface	"Configuring Single Sign-On using OracleAS SSO 10g" in <i>Oracle Fusion Middleware Application Security Guide</i>
Oracle IRM Desktop	Not supported
Oracle URM	"Configuring Single Sign-On using OracleAS SSO 10g" in <i>Oracle Fusion Middleware Application Security Guide</i>

4.12.3 Configuring Windows Native Authentication

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

Table 4–10 shows where to get more information about configuring WNA for Oracle ECM applications.

Table 4–10 WNA Configuration for Oracle ECM Applications

Application	Configuration Information
Oracle UCM Content Server	"Configuring Oracle UCM and Single Sign-On for Windows Native Authentication" in <i>Oracle Fusion Middleware System Administrator's Guide for Oracle Content Server</i>
Oracle I/PM	"Configuring Oracle UCM and Single Sign-On for Windows Native Authentication" in <i>Oracle Fusion Middleware System Administrator's Guide for Oracle Content Server</i>
Oracle IRM Web Interface	"Configuring Single Sign-On with Microsoft Clients" in <i>Oracle Fusion Middleware Securing Oracle WebLogic Server</i>
Oracle IRM Desktop	"Configuring Single Sign-On with Microsoft Clients" in <i>Oracle Fusion Middleware Securing Oracle WebLogic Server</i>
Oracle URM	"Configuring Single Sign-On with Microsoft Clients" in <i>Oracle Fusion Middleware Securing Oracle WebLogic Server</i>

4.13 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 *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 4–11](#) describes.

Table 4–11 Managed Servers, Clusters, and Machines Advanced Settings Screens

No.	Screen	Description and Action Required
1	Configure Managed Servers	Add new Managed Servers, or edit and delete existing Managed Servers. Click Next to continue.
2	Configure Clusters	Create clusters if you are installing in a high availability environment. For more information, see <i>Oracle Fusion Middleware High Availability Guide</i> . Click Next to continue.
3	Assign Servers to Clusters	If you configured any clusters on the Configure Clusters screen Click Next to continue.
4	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.
5	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.
6	Target Deployments to Clusters or Servers	Assign your Managed Servers to clusters or servers in your domain. Click Next to continue.
7	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 *Oracle Fusion Middleware Administrator's Guide*.

4.14 Setting Up Oracle Web Services Manager Security

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

1. [Installing Oracle WebLogic Server and Oracle Enterprise Content Management Suite](#)
2. [Creating an Oracle WSM MDS Schema with RCU](#)
3. [Configuring Oracle ECM 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](#)

4.14.1 Installing Oracle WebLogic Server and Oracle Enterprise Content Management Suite

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 3.1.2, "Installing Oracle WebLogic Server in a Middleware Home."](#)

The installation of Oracle WebLogic Server creates an Oracle Fusion Middleware home, where you can install Oracle Enterprise Content Management Suite, which creates an ECM Oracle home. Oracle WSM can be installed from the Oracle ECM suite. The Middleware home includes an Oracle Common home, where the Oracle WSM files are installed. For information about how to install Oracle Enterprise Content Management Suite, which installs the files necessary for deploying Oracle UCM to Oracle WebLogic Server, see [Section 3.2, "Installing Oracle Enterprise Content Management Suite in Oracle Fusion Middleware."](#)

4.14.2 Creating an Oracle WSM MDS Schema with RCU

Make the following selection on the Repository Creation Utility (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 Oracle UCM 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 Enterprise Content Management Suite Schemas."](#)

4.14.3 Configuring Oracle ECM Applications and Oracle WSM Policy Manager in an Oracle WebLogic Server Domain

To configure one or more Oracle ECM 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 4.2, "Creating an Oracle WebLogic Server Domain."](#) For information about extending a domain with Oracle WSM Policy Manager, see [Section 4.3, "Extending an Existing Domain."](#)

4.14.4 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 10.3, "Restarting a Managed Server."](#)

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

- [Section 5.2, "Completing the Initial Configuration of Oracle Content Server"](#)
- [Section 6.1, "Completing the Oracle IBR Configuration"](#)
- [Section 7.1, "Completing the Oracle I/PM Configuration"](#)
- [Section 8.1, "Performing Postinstallation Configuration"](#)
- [Section 9.1, "Completing the Oracle URM Configuration"](#)

4.14.5 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.

4.14.5.1 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/ECM_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 8.1.2, "Configuring a Key Store for Oracle IRM."](#)

4.14.5.2 Applying Oracle WSM Policies to Web Services

The following procedure shows how to apply a policy to the Oracle UCM web services `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 UCM 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`.

Configuring Oracle Universal Content Management

This chapter explains how to configure Oracle Universal Content Management (Oracle UCM) in an Oracle WebLogic Server domain, in these topics:

- [Completing the Oracle UCM Configuration](#)
- [Completing the Initial Configuration of Oracle Content Server](#)
- [Configuring Oracle Text Search for Oracle Content Server](#)
- [Configuring a JDBC Driver for Standalone Applications](#)
- [Importing a Database Root CA Certificate into the Key Store for a Standalone Application](#)
- [Enabling and Configuring Site Studio on Oracle Content Server](#)
- [Configuring Oracle Content Server for Desktop Integration Suite](#)
- [Installing and Configuring Desktop Integration Suite on a Client Workstation](#)
- [Opening Files from Microsoft Office 2010 Over a Non-SSL Connection](#)
- [Configuring Records Management in Oracle Content Server](#)
- [Configuring Oracle Application Extension Framework](#)
- [Installing and Configuring Oracle Document Capture and Oracle Distributed Document Capture](#)

5.1 Completing the Oracle UCM Configuration

After you start the Administration Server and Oracle UCM Managed Server, as described in [Chapter 10, "Verifying the Installation and Configuration,"](#) you can complete the Oracle UCM configuration on the postinstallation configuration page in Oracle Content Server.

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

`http://managedServerHost:managedServerPort/cs`

When you configure Oracle UCM on the same machine and in the same Oracle WebLogic Server domain as Oracle I/PM, the postinstallation configuration of Oracle UCM is done automatically. If you follow the default configuration for the installation of Oracle UCM and Oracle I/PM, both applications are installed on the same machine. In this environment, Oracle I/PM provides a configuration file to Oracle UCM that sets up Oracle UCM for use by Oracle I/PM.

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

The Oracle I/PM administrator should verify that the default Oracle UCM configurations are correct for use by the Oracle I/PM Managed Server. For Oracle I/PM use, many of the Oracle UCM postinstallation configuration steps, such as configuring Oracle Inbound Refinery, are not required.

Before you can use Oracle Inbound Refinery (Oracle IBR) with Oracle UCM, you need to configure Oracle IBR for document and image conversions to work with Oracle 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 4.7.2, "Setting Library Paths in Environment Variables on UNIX Platforms."](#)

To complete the Oracle UCM configuration:

1. Start the Administration Server, as described in [Chapter 10.1, "Starting the Administration Server."](#)
2. Start the Oracle UCM Managed Server, as described in [Chapter 10.2, "Starting Managed Servers."](#)
3. Browse to the Oracle Content Server postinstallation configuration page, at this web site:

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

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.

For information about the values to enter, see [Section 5.2, "Completing the Initial Configuration of Oracle Content Server."](#)

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

`127.0.0.1your.server.IP.address|0.0.0.0.0.0.1|`

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 Oracle Content Server.

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

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

For more information, see [Section 4.14.4, "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 Oracle IBR back to Oracle 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 Oracle Content Server.

7. Click **Submit**.
8. Restart Oracle Content Server, as described in [Section 10.3, "Restarting a Managed Server."](#)

5.2 Completing the Initial Configuration of Oracle Content Server

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

- [Starting Oracle Content Server](#)
- [Configuring the Oracle Content Server Instance](#)
- [Configuring Oracle Content Server for IBM DB2 Database Searches](#)

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

5.2.1 Starting Oracle Content Server

You can start an Oracle UCM instance, which includes Oracle 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 Oracle Content Server" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Content Server*.

5.2.2 Configuring the Oracle Content Server Instance

[Figure 5–1](#) shows the configuration page for Oracle Content Server.

Figure 5-1 Configuration Page for Oracle Content Server

Content Server Configuration

Node Information

Cluster Node Identifier: ⓘ UCM_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_
Content Server URL Prefix: ⓘ /cs/

Instance Information

Is New Content Server Instance: ⓘ
Server Socket Port: ⓘ
Incoming Socket Connection Address Security Filter: ⓘ 127.0.0.1|192.0.2.236|0.0.0.0.0.0.1
* Web Server HTTP/HTTPS Address: ⓘ myhost.example.com:16202
Web Address Is HTTPS: ⓘ
Company Mail Server: ⓘ mail
Administrator E-Mail Address: ⓘ sysadmin@example.com
* Server Instance Name: ⓘ myhost_4444
* Server Instance Label: ⓘ myhost_4444
* Server Instance Description: ⓘ Instance myhost_4444
Is Auto Number Enabled: ⓘ
Auto Number Prefix: ⓘ myhost_444

Search Information

FullText Search Option: ⓘ None ▼
External DataSource: ⓘ

* - Required

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

Field	Description
Cluster Node Identifier	The name of the Oracle UCM Managed Server where Oracle Content Server will run.
Content Server Instance Folder	<p>The absolute path to the Oracle instance directory of Oracle Content Server, which is <i>DomainHome/ucm</i> by default.</p> <p>The default Oracle instance directory for Oracle Content Server follows:</p> <pre>MW_HOME/user_projects/domains/DomainHome/ucm/cs</pre> <p>The name of the top-level folder in the folder hierarchy for the Oracle Content Server instance is <i>cs</i>.</p> <p>The path to the Oracle instance directory is the value of the <code>IntradocDir</code> variable for the Oracle 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.</p>
Native File Repository Location	The path to the vault directory for storing native content checked into Oracle 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 Oracle Content Server instance.
Is New Content Server Instance	Whether or not the Oracle Content Server instance is a new one.
Server Socket Port	<p>The number of the port for calling top-level services. The default value is <code>blank</code>.</p> <p>Changing this field value changes the <code>IntradocServerPort</code> entry in <code>DomainHome/ucm/cs/config/config.cfg</code>. The default <code>IntradocServerPort</code> value is <code>blank</code>.</p>
Incoming Socket Connection Address Security Filter	<p>Restricts Oracle Content Server access to a computer or computers with a specified IP address or addresses.</p> <ul style="list-style-type: none"> ■ By default, this field is prefilled with the IP address of the local host (<code>127.0.0.1</code>). ■ You can specify multiple IP addresses, separated by pipes (<code> </code>). Make sure that there are no spaces on either side of the pipe character. (For example: <code>127.0.0.1 0:0:0:0:0:0:0:1 192.168.1.1</code>) ■ You can use wildcards in this field, <code>*</code> for zero or many characters, and <code>?</code> for any one character. (For example, <code>10.10.3.*</code>) ■ 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. (<code>HttpServerAddress</code> property).

Field	Description
Web Address Is HTTPS	Whether or not the URL for the web server starts with HTTPS, for a Managed Server that has SSL enabled.
Company Mail Server	An email server that Oracle Content Server can use to send email notifications. This value generally takes the form of <i>mail.company.com</i> . If applicable, make sure to allow for sending email through a firewall.
Administrator E-Mail Address	An email address that Oracle Content Server can use to send email notifications (<i>SysAdminAddress</i>). This address will receive a returned message for any delivery failure that occurs.
Server Instance Name	The name of the Oracle Content Server instance.
Server Instance Label	The instance name that is displayed in the Windows Start menu (<i>InstanceMenuLabel</i> property).
Server Instance Description	A description of the Oracle Content Server instance (<i>InstanceDescription</i> property).
Is Auto Number Enabled	Whether or not automatic numbering of Oracle Content Server instances is enabled.
Auto Number Prefix	A unique prefix for an Oracle Content Server instance number, to avoid conflicts among multiple Oracle Content Server instances (<i>Auto Number Prefix</i> system property).
FullText Search Option	Specifies the search engine for full-text searches: <ul style="list-style-type: none"> ■ None: The Oracle Content Server instance will use <code>DATABASE.METADATA</code> as the search engine. ■ Internal: For Oracle Database, the Oracle Content Server instance will use <code>OracleTextSearch</code> with the system database. For Microsoft SQL Server, it will use <code>DATABASE.FULLTEXT</code>. ■ External: The Oracle Content Server instance will use <code>OracleTextSearch</code> with an external data source for an Oracle Database (not the system database). If you select this option, you must provide the name of the external data source in the External DataSource field.
External DataSource	The name of an external data source that was created through the Administration Console and targeted to the Oracle UCM Managed Server, using an <code>OCSSEARCH</code> 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 <i>Oracle Fusion Middleware Java EE Developer's Guide for Oracle Application Development Framework</i> . You can specify the name of an external provider for the data source. For information about creating an external provider, see Section 5.3.2, "Configuring an External Database Provider for Standalone Applications." If the external data source is for use with IBM DB2, also see Section 5.2.4, "Configuring Oracle Content Server for IBM DB2 Database Searches." For information about the <code>OCSSEARCH</code> schema, see Section 2.2, "Creating Oracle Enterprise Content Management Suite Schemas."

5.2.3 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 Oracle 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, which displays lists of enabled and disabled server components, click **advanced component manager**.
4. You can select individual components in the tables 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.

5.2.4 Configuring Oracle Content Server for IBM DB2 Database Searches

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

To configure IBM DB2 database searches in Oracle Content Server:

1. Open a new browser window, and log in to Oracle 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 an Oracle Content Server instance.

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

4. In the option list for the Oracle 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 Oracle Content Server, as described in [Section 10.3, "Restarting a Managed Server."](#)

5.2.5 Configuring Microsoft SQL Server to Work with Oracle UCM

Before you can use Microsoft SQL Server with Oracle UCM, you need to turn on snapshot isolation in the database. If you plan to use SQL Server for the back-end database for Oracle Imaging and Process Management (Oracle I/PM) 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 Oracle UCM 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 [Section 2.2, "Creating Oracle Enterprise Content Management Suite Schemas."](#)

For more information about supported databases, see [Section 2.1.1, "Database Prerequisites."](#)

5.3 Configuring Oracle Text Search for Oracle Content Server

The Oracle Text Search feature enables the use of Oracle Text 11g as the primary full-text search engine for Oracle UCM. Oracle Text 11g offers state-of-the-art indexing capabilities and provides the underlying search capabilities for Oracle Secure Enterprise Search (Oracle SES).

Oracle Text Search enables administrators to specify certain metadata fields to be optimized for the search index as well as to customize additional fields. This feature also enables a fast index rebuild and index optimization.

Before you can use Oracle Text Search, you need to run Repository Creation Utility (RCU) to create a search schema (*prefix_OCSSEARCH*) in an Oracle Database instance, create a data source that points to the search schema, and then use the Administration Console to target the data source to the Oracle UCM Managed Server (`UCM_server1` by default). For information about creating a schema, see [Chapter 2, "Creating Schemas for Oracle Enterprise Content Management Suite."](#)

To search auxiliary metadata in Oracle URM with Oracle Text, you must configure Oracle Content Server to use Oracle Text Search as the search engine. You can set Oracle Text Search on the Oracle UCM postinstallation configuration page or in the configuration file. You can change the configuration of the full-text search option to Oracle Text Search in the `config.cfg` configuration file.

Oracle Text Search supports the use of Oracle Secure Enterprise Search (Oracle SES) 11g as the primary full-text search engine for Oracle UCM. If you have a license to use Oracle SES, you can configure it for use with Oracle Text Search on Oracle UCM and configure Oracle Content Server to use Oracle SES as its back-end search engine. For more information, see "Oracle Secure Enterprise Search" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Content Server*.

You can configure Oracle Text Search on the postinstallation configuration page for Oracle Content Server, which [Figure 5-1](#) shows, by selecting `Internal` or `External` in the **FullText Search Option** field. If you select the `External` option, you must provide the name of the external data source in the **External DataSource** field. For more information about these fields, see [Section 5.2.2, "Configuring the Oracle Content Server Instance."](#)

If you did not configure Oracle Text Search on the configuration page for Oracle Content Server, you can configure this search option in the `config.cfg` configuration file for the Oracle Content Server instance. You can also change the search option in this file. After changing the search option, you need to restart Oracle Content Server and rebuild the search index.

To configure Oracle Text Search for Oracle Content Server in the configuration file:

1. Open the `config.cfg` file for the Oracle Content Server instance in a text editor.
2. Set the following property value:

```
SearchIndexerEngineName=OracleTextSearch
```

3. If you are using an external data source instead of the system database, change `SystemDatabase` in the following property to the external data source name:

```
IndexerDatabaseProviderName=SystemDatabase
```

Note: You can specify a separate Oracle Database as the value of `IndexerDatabaseProviderName`, instead of `SystemDatabase`. However, before Oracle Text Search can function properly with the separate Oracle Database, you need to manually copy the `ojdbc14.jar` file from the `ECM_ORACLE_HOME/ucm/idc/shared/classes` folder to the `UCM_DOMAIN/config/lib` folder.

4. Save the file.
5. Restart Oracle Content Server, as described in [Section 10.3, "Restarting a Managed Server."](#)
6. Rebuild the search index.

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

5.3.1 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 11g:

- 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 *OracleMetaLink*) web site at <http://support.oracle.com>
2. To apply each patch, follow the instructions in its Read Me document.

5.3.2 Configuring an External Database Provider for Standalone Applications

You can create an external database provider in Oracle 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 Oracle Text Search, 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 *Oracle Fusion Middleware System Administrator's Guide for Oracle Content Server*.

5.4 Configuring a JDBC Driver for Standalone Applications

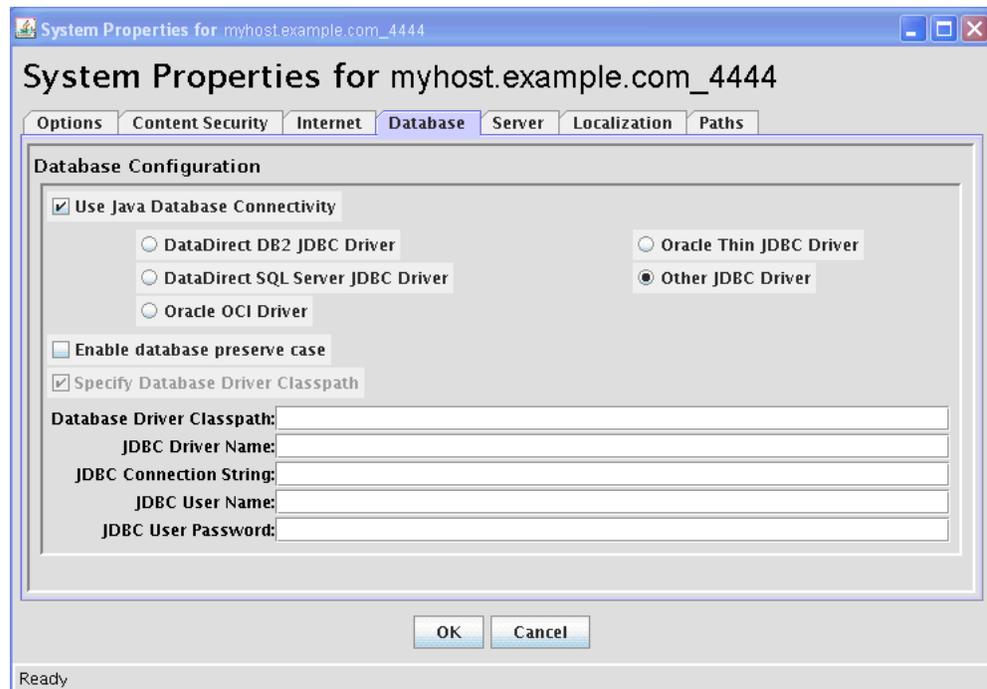
For Oracle Content Server to work with standalone applications, such as the Batch Loader Utility, you need to configure a JDBC driver for the system database or an external database provider. Oracle Fusion Middleware provides DataDirect JDBC drivers for Microsoft SQL Server and IBM DB2 databases to support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

To configure a JDBC Driver for standalone applications:

1. As a system administrator, run `SystemProperties` from the `bin` directory for the Oracle Content Server instance.
 - **UNIX path:** `DomainHome/ucm/cs/bin/SystemProperties`
 - **Windows path:** `DomainHome\ucm\cs\bin\SystemProperties`

The System Properties utility starts.

Figure 5–2 System Properties Utility



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 Oracle Content Server, as described in [Section 10.3, "Restarting a Managed Server."](#)

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

Oracle 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_20_D1.1.0-2119\bin\keytool -import -trustcacerts
  -alias dbroot -keystore
c:\mw_home\jrockit_160_20_D1.1.0-2119\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.mydomain.com)
(PORT=2490
))) (CONNECT_DATA=(SERVICE_NAME=orcl.us.oracle.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.

5.6 Enabling and Configuring Site Studio on Oracle Content Server

Before you can use Site Studio, you need to complete some configuration steps in Oracle Content Server. You can configure Site Studio on Oracle Content Server after you install the Oracle UCM 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 Oracle Content Server. For more information, see [Section 5.6.1, "Enabling Site Studio on Oracle Content Server."](#)

The Site Studio Designer installer can be downloaded from the **My Content Server** tray or menu, under **My Downloads**. For information about using this application, see the *Oracle Fusion Middleware 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 Oracle 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 Fusion Middleware 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 Universal Content Management 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 Oracle 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 Oracle Content Server](#)
- [Setting Default Project Document Information](#)
- [Setting Default Metadata for Web Site Assets](#)
- [Configuring Zone Fields](#)
- [Enabling JavaServer Pages on Oracle Content Server](#)
- [Rebuilding the Oracle 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 11g Site Studio site running on Oracle WebLogic Server and use an Oracle UCM 10gR3 server as the back end. For information about using Site Studio 11gR1 (11.1.1.4.0) with Oracle UCM 10gR3, see "Configuring Oracle Content Server 10gR3 for Use with Site Studio 11gR1" in the *Oracle Fusion Middleware Technical Reference Guide for Site Studio*.

5.6.1 Enabling Site Studio on Oracle Content Server

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

To enable Site Studio on Oracle Content Server:

1. Log in to Oracle UCM as an administrator.
2. In the Oracle Content Server **Administration** tray, click **Admin Server**.
3. On the Oracle 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 Oracle Content Server, as described in [Section 10.3, "Restarting a Managed Server."](#)

5.6.2 Setting Default Project Document Information

When you create a new web site in Site Studio, a new project file is created and checked into Oracle 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 Oracle Content Server.

To set the default project document information:

1. Log in to Oracle 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.

5.6.3 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 Oracle Content Server. You can set this default metadata on the Set Default Web Asset Document Information page, available through the Oracle Content Server **Administration** tray or menu under **Site Studio Administration**.

For information about setting default metadata for Site Studio web site assets, see Section A.8, "Set Default Web Asset Document Information Page," in *Oracle Fusion Middleware Administrator and Manager's Guide for Site Studio*.

5.6.4 Configuring Zone Fields

The Site Studio component uses several metadata fields that are added to Oracle Content Server. If you do not use Oracle Text Search, 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 Oracle 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 5.6, "Enabling and Configuring Site Studio on Oracle 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 Oracle UCM as an administrator.
2. In the Oracle 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.

5.6.5 Enabling JavaServer Pages on Oracle Content Server

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

Important:

- JSP is supported only in legacy Site Studio projects; that is, projects that use the pre-10gR4 architecture. These are typically projects that were created in a Site Studio release before 10gR4 and that are opened in Designer 11gR1.
 - You cannot enable JSP on Oracle Content Server and then use Site Studio for External Applications remote templates in the same security group. If you did, Oracle 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 Oracle 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 10gR3 documentation set.

To configure JSP Support for a new JSP group

1. Log in to Oracle UCM 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 Oracle Content Server.

5.6.6 Rebuilding the Oracle 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 Oracle 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 Oracle 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 Oracle Content Server instance. You should perform this rebuild during off-peak hours of Oracle 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 *Oracle Fusion Middleware Technical Reference Guide for Site Studio*), you must rebuild the search index on Oracle 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 *Oracle Fusion Middleware System Administrator's Guide for Oracle Content Server*.

5.7 Configuring Oracle Content Server for Desktop Integration Suite

Before clients can use Desktop Integration Suite (DIS) with Oracle Content Server, make sure the `CoreWebDAV` component is enabled, if not already enabled, and enable the `Folders_g` and `DesktopTag` components.

You might also want to enable `EmailMetadata`, which maps email message fields to email metadata fields, and `RMAEmail`, which provides email metadata fields and distribution lists.

To configure Oracle Content Server for Desktop Integration Suite:

1. In the Oracle Content Server **Administration** tray, click **Admin Server**.
2. In the Admin Server Component Manager, select **Folders**.
3. If `CoreWebDAV` is not already enabled, select it.
4. Select `Folders_g`, `DesktopTag`, and, optionally, the `EmailMetadata` and `RMAEmail` components.
5. Click the **Update** button.
6. Click the **OK** button to enable these components.
7. Restart Oracle Content Server, as described in [Section 10.3, "Restarting a Managed Server."](#)

5.8 Installing and Configuring Desktop Integration Suite on a Client Workstation

Desktop Integration Suite provides a set of embedded applications that help users seamlessly integrate their desktop experiences with Oracle 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 the Desktop Integration Suite on a client workstation, see "Setting Up Desktop Integration on Client Computers" in *Oracle Fusion Middleware User's Guide for Desktop Integration Suite*.

5.9 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>

5.10 Configuring Records Management in Oracle Content Server

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

Note: If you do not want to use Records Management in Oracle Content Server, you can remove the configuration user interface by disabling the `RMFeatureConfig` component. For more information, see [Section 5.2.3, "Enabling or Disabling Components."](#)

Before you disable Records Management and restart Oracle Content Server, you need to delete the Report template files that Records Management installs. You cannot delete them after Records Management is disabled.

To configure Records Management in Oracle 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, and then click **Submit**:
 - **None**
 - **Standalone**
 - **Adapter**

3. Restart Oracle UCM, as described in [Section 10.3, "Restarting a Managed Server."](#)

Whenever the screen says to restart the server during the Records Management configuration, restart the Oracle UCM Managed Server.

4. After you restart Oracle UCM, the Records Management Setup Checklist is displayed again.

For information about completing items on the Setup Checklist, see [Section 9.1.2, "Completing the Setup Checklist for Oracle URM."](#)

5. 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 Oracle URM 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 Oracle URM 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 Oracle URM Managed Server
- Validate the specified source values

Compare the retention schedules of the adapter and the Oracle URM Managed Server to determine whether any items in the adapter are not in the Oracle URM 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 Oracle URM 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 Oracle URM server, and the backups are checked into Oracle 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.

6. 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 Oracle Content Server. You can use the same name for each field as defined in Oracle Content Server, or you can rename the field to something different. When the content is uploaded to the Oracle URM 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.

7. After Records Management is initially configured on Oracle 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 Fusion Middleware Setup Guide for Universal Records Management*.

8. 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 Oracle URM server; otherwise, an error occurs. For more information about the Features and Disposition Actions sections of the Enabled Features page, see [Section 9.1.1, "Enabling Oracle URM Components."](#)

After you change any features or dispositions, restart Oracle UCM, as described in [Section 10.3, "Restarting a Managed Server."](#)

5.11 Configuring Oracle Application Extension Framework

Oracle Application Extension Framework (AXF) is automatically installed with Oracle I/PM. For information about verifying the installation, see [Section 7.5, "Installing and Configuring Oracle Application Extension Framework."](#)

For information about configuring and using AXF and the AXF database tables, see *Oracle Fusion Middleware E-Business Suite Adapter for Oracle Enterprise Content Management Administrator's Guide* or *Oracle Fusion Middleware Administrator's Guide for Oracle PeopleSoft Adapter for Oracle Enterprise Content Management*.

5.12 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 *Oracle Document Capture Installation Guide* and *Oracle Document Capture Administrator's Guide*.

For information about installing and configuring Oracle Distributed Document Capture, see *Oracle Distributed Document Capture Installation Guide* and *Oracle Distributed Document Capture Administrator's Guide*.

The Oracle UCM 11g Commit Driver is required to commit documents from either capture application to Oracle UCM. For information about using the Oracle UCM 11g Commit Driver, see *Oracle Distributed Document Capture Installation Guide* or *Oracle Distributed Document Capture Administrator's Guide*.

Configuring Oracle Inbound Refinery

This chapter explains how to configure Oracle Inbound Refinery (Oracle IBR) on a Managed Server in an Oracle WebLogic Server domain, in these topics:

- [Completing the Oracle IBR Configuration](#)
- [Installing and Configuring Oracle IBR on Oracle UCM](#)

6.1 Completing the Oracle IBR Configuration

Before you can use Oracle Inbound Refinery with Oracle Universal Content Management (Oracle UCM), you need to complete the configuration of Oracle IBR for document and image conversions to work with Oracle 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 Oracle IBR Managed Server. For more information, see [Section 4.7.2, "Setting Library Paths in Environment Variables on UNIX Platforms."](#)

To complete the Oracle IBR configuration:

1. Start the Administration Server and the Oracle IBR and Oracle UCM Managed Servers, as described in [Chapter 10, "Verifying the Installation and Configuration."](#)
2. Configure Oracle Content Server, as described in [Section 5.1, "Completing the Oracle UCM Configuration."](#)
3. Browse to the Oracle IBR postinstallation configuration page, at this web site:
`http://managedServerHost:16250/ibr/`
4. Enter or edit all necessary values.
 - To enable access from Oracle 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 Oracle Content Server instance or instances that will send jobs to Oracle IBR, not the IP address of Oracle IBR. (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 Oracle IBR.

Note: The **Incoming Socket Connection Address Security Filter** value must be set correctly for Oracle IBR to be usable.

- In the **Server Socket Port** field, if you want to set up a provider from Oracle IBR back to Oracle 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 Oracle IBR to be usable.

5. Restart Oracle IBR, as described in [Section 10.3, "Restarting a Managed Server."](#)
6. Check all the entries in `DomainHome/ucm/ibr/config/config.cfg` have the values that you want for the Oracle IBR configuration.

6.2 Installing and Configuring Oracle IBR on Oracle UCM

Oracle 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, Oracle IBR 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 Oracle IBR to convert content items stored in Oracle Content Server.

The installation and configuration of Oracle ECM includes Oracle IBR. Before you can use Oracle IBR with Oracle UCM, you need to complete the configuration for document and image conversion to work with Oracle Content Server. To complete the configuration, perform these tasks:

- [Configuring Oracle IBR on Oracle UCM](#)
- [Configuring Document Conversion on Oracle IBR](#)
- [Setting Up Oracle Content Server to Send Jobs to Oracle IBR for Conversion](#)

6.2.1 Configuring Oracle IBR on Oracle UCM

Oracle IBR has a postinstallation configuration page that you need to complete after the configuration of Oracle Content Server.

To configure Oracle IBR on Oracle UCM:

1. Configure Oracle Content Server, as described in [Section 5.2, "Completing the Initial Configuration of Oracle Content Server."](#)
2. Browse to the Oracle IBR postinstallation configuration page, at this web site:

`http://managedServerHost:16250/ibr/`

[Figure 6–1](#) shows the Inbound Refinery Configuration page for postinstallation configuration.

Figure 6–1 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 6–1 shows.

Field	Description
Inbound Refinery Instance Folder	<p>The absolute path to the Oracle instance directory of Oracle Inbound Refinery, which is <i>DomainHome</i>/ucm/by default.</p> <p>The default Oracle instance directory for Oracle IBR follows: <code>MW_HOME/user_projects/domains/DomainHome/ucm/ibr</code></p> <p>The name of the top-level folder in the folder hierarchy for the Oracle Content Server instance is <code>ibr</code>.</p> <p>The path to the Oracle instance directory is the value of the <code>IntradocDir</code> variable for the Oracle IBR 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.</p>
Native File Repository Location	The path to the vault directory for storing native content.
Weblayout Folder	The path to the weblayout directory for storing web-viewable renditions of native and alternate files.
Register Start Menu Actions	Whether or not the Start Menu actions will be registered.

Field	Description
Server Socket Port	<p>If you want to set up a provider from Oracle IBR back to Oracle Content Server, enter an unused port number, such as 4444, for Server Socket Port.</p> <p>This value is the number of the port for calling top-level services. Changing this field value changes the <code>IntradocServerPort</code> entry in <code>DomainHome/ucm/ibr/config/config.cfg</code>.</p> <p>Note: The Server Socket Port value must be set correctly for Oracle IBR to be usable.</p>
Incoming Socket Connection Address Security Filter	<p>Restricts Oracle IBR access to a computer or computers with a specified IP address or addresses.</p> <p>To enable access from Oracle Content Server, provide a value for this field as follows:</p> <pre>127.0.0.1 0:0:0:0:0:0:1 your.server.IP.address</pre> <p>This value should be the IP address of the Oracle Content Server instance or instances that will send jobs to Oracle IBR, not the IP address of Oracle IBR. (In a test or demo environment, these IP addresses could be the same.)</p> <p>This field accepts wildcards in the value, like <code>10.*.*.*</code>. You can change this value later by setting <code>SocketHostAddressSecurityFilter</code> in <code>DomainHome/ucm/ibr/config/config.cfg</code> and restarting Oracle IBR.</p> <p>Note: The Incoming Socket Connection Address Security Filter value must be set correctly for Oracle IBR to be usable.</p>
Web Server HTTP/HTTPS Address	The name of the web server. (<code>HttpServerAddress</code> property).
Web Address Is HTTPS	Whether or not the URL for the web server starts with <code>HTTPS</code> , for a server that has SSL enabled.
Inbound Refinery URL Prefix	The relative URL for the Oracle IBR instance.
Server Instance Name	The name of the Oracle IBR instance.
Server Instance Label	The instance name that is displayed for Oracle IBR.
Server Instance Description	A description of the Oracle IBR instance.

- Restart Oracle Inbound Refinery, as described in [Section 10.3, "Restarting a Managed Server."](#)
- Restart Oracle Content Server.

You can restart an Oracle Content Server instance by restarting the Oracle UCM 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 10.3, "Restarting a Managed Server."](#)

After you restart the Oracle UCM Managed Server, you can set up Oracle Inbound Refinery and Oracle Content Server for document conversion. The core Oracle IBR uses Outside In technology to convert native documents to web-viewable PDF files or JPEG thumbnails. Other conversions require additional Oracle IBR components. These components are installed but disabled on Oracle IBR 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 Oracle Content Server.

For many conversions, Oracle IBR needs access to a directory with usable fonts. On a Windows operating system, the default Windows fonts in C:\WINDOWS\FONTS will work. On a UNIX operating system, you must provide your own path. For more information, see [Section 4.6, "Setting Up Fonts on a UNIX System."](#)

On Oracle Content Server, you must set up an outgoing provider from Oracle Content Server to Oracle IBR, with the **Handles Inbound Refinery Conversion Jobs** option checked, as described in [Section 6.2.3.1, "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 Oracle Content instance. If this component is not enabled, you must enable it on any Oracle Content Server instance that will use Oracle IBR for document conversion, as described in [Section 6.2.2.1, "Enabling Conversion Components on Oracle IBR."](#)

6.2.2 Configuring Document Conversion on Oracle IBR

To configure document conversion on Oracle IBR, perform these tasks:

- [Enabling Conversion Components on Oracle IBR](#)
- [Enabling PDFExportConverter in Oracle IBR](#)

6.2.2.1 Enabling Conversion Components on Oracle IBR

The core IBR 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 *Oracle Fusion Middleware Administrator's Guide for Conversion*.

To enable conversion components on Oracle IBR:

1. From the Oracle IBR **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 Oracle IBR, as described in [Section 10.3, "Restarting a Managed Server."](#)

For more information, consult the `readme` files and the documentation for each component.

6.2.2.2 Enabling PDFExportConverter in Oracle IBR

`PDFExportConverter` uses `OutsideIn` 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 Oracle IBR as a server feature.

To enable PDFExportConverter on Oracle IBR:

1. From the Oracle IBR **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 Oracle IBR, as described in [Section 10.3, "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 *Oracle Fusion Middleware Administrator's Guide for Conversion*.
7. Make sure that file formats are configured on Oracle Content Server to be sent to Oracle IBR, as described in [Section 6.2.3.3, "Selecting File Formats To Be Converted."](#)

6.2.3 Setting Up Oracle Content Server to Send Jobs to Oracle IBR for Conversion

Before Oracle Content Server can send jobs to Oracle IBR for conversion, you need to perform these setup tasks:

- [Creating an Outgoing Provider](#)
- [Enabling Components for Oracle IBR on Oracle Content Server](#)
- [Selecting File Formats To Be Converted](#)

6.2.3.1 Creating an Outgoing Provider

Before Oracle Content Server can send files to Oracle IBR for conversion, you must set up an outgoing provider from Oracle Content Server to Oracle IBR with the **Handles Inbound Refinery Conversion Jobs** option checked.

To create an outgoing provider:

1. From the Oracle 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 Oracle IBR instance is running, such as `myhost.us.example.com:16250`.
 - **HTTP Server Address:** The address of the Oracle IBR instance, such as `myhost.example.com:16250`.
 - **Server Port:** The value that was entered in the **Server Socket Port** field (`IntradocServerPort` value) for the Oracle IBR instance. This value is the number of the port for calling top-level services.

You can find this value on the Oracle IBR configuration information page, as follows:

- a. From the Oracle IBR **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 Oracle IBR (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 Oracle IBR configuration information page, as follows:

- a. From the Oracle IBR **Administration** menu, select **Configuration Information**.
 - b. Look for the **Server Name**, value.
- **Relative Web Root:** The web root of the Oracle IBR 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 Oracle Content Server, as described in [Section 10.3, "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 Oracle Content Server and Oracle IBR instances can ping each other.

For more information about setting up providers, see "Configuring Content Server and Refinery Communication" in *Oracle Fusion Middleware Administrator's Guide for Conversion*.

6.2.3.2 Enabling Components for Oracle IBR on Oracle Content Server

Some conversion types require *helper* components to be enabled on Oracle Content Server. The `InboundRefinerySupport` component must always be enabled on any Oracle Content Server instance that uses IBR for document conversion. It is enabled by default on a new Oracle Content Server installation.

To enable components for Oracle IBR on Oracle Content Server:

1. From the Oracle 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 Oracle Content Server, as described in [Section 10.3, "Restarting a Managed Server."](#)

6.2.3.3 Selecting File Formats To Be Converted

To tell Oracle Content Server which files to send to IBR to be converted, you need to select file formats.

To select file formats to be converted:

1. From the Oracle Content Server **Administration** menu, choose **Refinery Administration** and then **File Formats Wizard**.

Oracle Content Server displays the File Formats Wizard page. This page configures what file formats will be sent to Oracle Inbound Refinery for conversion when they are checked into Oracle 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 *Oracle Fusion Middleware Administrator's Guide for Conversion*.

Configuring Oracle Imaging and Process Management

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

- [Completing the Oracle I/PM Configuration](#)
- [Configuring the Full-Text Features in the Oracle UCM Repository](#)
- [Connecting to a Workflow Server](#)
- [Setting Oracle I/PM System Security](#)
- [Installing and Configuring Oracle Application Extension Framework](#)
- [Installing and Configuring Oracle Document Capture and Oracle Distributed Document Capture](#)

7.1 Completing the Oracle I/PM Configuration

Before you complete the configuration of Oracle I/PM, your system needs to have Universal Content Management (Oracle UCM) installed and configured. Oracle I/PM uses Oracle UCM for its repository. You can use either Oracle UCM 11g or Oracle UCM 10g as the Oracle I/PM repository. For information about configuring Oracle UCM 11g, see [Chapter 4, "Configuring Oracle Enterprise Content Management Suite,"](#) [Chapter 5, "Configuring Oracle Universal Content Management,"](#) and [Section 7.1.1.1, "Configuring Oracle Content Server 11g to Work with Oracle I/PM."](#) For information about using Oracle UCM 10g as the repository, see [Section 7.1.1.2, "Installing and Configuring Oracle UCM 10g to Work with Oracle I/PM."](#)

Note: In a production system, Oracle Enterprise Content Management Suite applications need to use an external Lightweight Directory Application Protocol (LDAP) authentication provider rather than the Oracle WebLogic Server embedded LDAP server, which is part of the default configuration. If you want to reassociate the identity store for Oracle I/PM with an external LDAP authentication provider, it is easier to do this before you complete the configuration of the Oracle I/PM Managed Server and before you connect it to the Oracle Universal Content Management (Oracle UCM) repository. For more information, see [Section 4.9, "Reassociating the Identity Store with an External LDAP Authentication Provider."](#)

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

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

1. [Configuring an Oracle UCM Repository for Oracle I/PM](#)
2. Starting the Administration Server and the Oracle UCM Managed Server, as described in [Chapter 10, "Verifying the Installation and Configuration"](#)
3. [Starting the Oracle I/PM Managed Server and Accessing the Web Client](#)
4. [Connecting to an Oracle UCM Repository](#)
5. [Configuring the GDFontPath MBean for a UNIX System](#)
6. [Allowing IMPORT Definitions](#)

7.1.1 Configuring an Oracle UCM Repository for Oracle I/PM

You can configure either Oracle Content Server 11g or Oracle Content Server 10g as the Oracle UCM Repository for Oracle I/PM.

Note: You will not be able to import or upload content to the Oracle I/PM system unless you have created a repository connection.

7.1.1.1 Configuring Oracle Content Server 11g to Work with Oracle I/PM

Oracle UCM 11g is installed with Oracle Enterprise Content Management Suite. When an Oracle UCM Managed Server and Oracle I/PM Managed Server are configured in an Oracle WebLogic Server domain on the same host machine, the configuration of Oracle Content Server 11g to work with Oracle I/PM is automatic.

If Oracle UCM is installed in a domain that is later extended with Oracle I/PM, then Oracle UCM will not be reconfigured to work with Oracle I/PM until the next restart of the Oracle UCM Managed Server. In this case, you must restart the Oracle UCM Managed Server, as described in [Section 10.3, "Restarting a Managed Server,"](#) before connecting to Oracle Content Server from the Oracle I/PM web client, as described in [Section 7.1.3, "Connecting to an Oracle UCM Repository."](#)

If the Oracle UCM and Oracle I/PM Managed Servers are configured to run on different machines, configuring Oracle I/PM will not configure Oracle UCM 11g to work with it. In this case, you must follow the manual configuration steps to configure Oracle UCM.

To configure Oracle UCM 11g manually to work with Oracle I/PM:

1. Start the Oracle UCM Managed Server, as described in [Section 10.2, "Starting Managed Servers."](#)
2. Access Oracle Content Server, as described in [Section 5.2.1, "Starting Oracle 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 Oracle Content Server.

- d. Click the **OK** button to enable this feature.
- e. Restart Oracle Content Server, as described in [Section 10.3, "Restarting a Managed Server."](#)

If **IpmRepository** was already selected, you do not need to restart the server.

7.1.1.2 Installing and Configuring Oracle UCM 10g to Work with Oracle I/PM

For an Oracle UCM 10g repository, Oracle I/PM requires Oracle Universal Content Management (Oracle UCM) 10gR3 (10.1.3.3.3), also referred to as Oracle Content Server 10gR3. After installing and configuring Oracle Content Server 10gR3, you need to update the system with the Content Server 10g Update Bundle. Both are required for Oracle UCM 10g to work with Oracle I/PM 11g.

You can download both Oracle Content Server 10gR3 and the Content Server 10g Update Bundle from Oracle E-Delivery or Oracle Technology Network (OTN). For more information about the software locations, see [Section 1.2, "Software Downloads for Oracle ECM Installation and Configuration."](#)

For information about installing and configuring Oracle Content Server 10gR3, see the Oracle Content Server page on Oracle Technology Network at

<http://www.oracle.com/technetwork/middleware/content-management/cs-088869.html>

If you are using Oracle I/PM 11g with Oracle Content Server 10gR3, make sure to update Oracle Content Server with the latest update patch.

7.1.1.2.1 Upgrading the JDK Version of Oracle Content Server 10g After you deploy Oracle I/PM 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 10gR3 (Oracle UCM) installation to the same JDK 1.6 version that Oracle I/PM uses. This is the JDK version that you specified for the Oracle I/PM Managed Server on the Configure Server Start Mode and JDK screen of the Fusion Middleware Configuration Wizard. For information about the JDK version that Oracle I/PM 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 Oracle Imaging and Process Management and Oracle Information Rights Management 11gR1 (xls)**.

For information about changing the JDK version that Oracle Content Server 10gR3 uses, see *Oracle Universal Content Management Content Server Installation Guide*, version 10gR3, for your operating system.

7.1.1.2.2 Configuring Oracle Content Server 10g to Work with Oracle I/PM You need to configure Oracle Content Server before it can work with Oracle I/PM. During the configuration, restart Oracle Content Server whenever prompted to do so.

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

1. Update the IP address filter:
 - a. On the system where Oracle UCM 10g 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 Oracle I/PM is installed.

 For example: `192.0.2.1|192.0.2.130`

 The IP address is required for the Oracle I/PM system to have access to the Oracle UCM system without authentication.
 - d. Click **OK**.

 This change will require a restart of Oracle Content Server, which you can do at the end of this procedure, after installing the Oracle UCM components.
2. Open the Oracle UCM web client in a web browser (`http://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 does the upgrade automatically.

Oracle I/PM content is not accessible in a web store. Oracle Content Server traditionally uses a `weblayout` directory on a file system to store content in a format for viewing in a web browser, but this feature does not have much use in an Oracle I/PM solution and uses extra disk space. After the file store upgrade, you should disable the `weblayout` functionality in Oracle Content Server for any file store provider configured for use as an Oracle I/PM volume.
5. Configure system properties:
 - a. Confirm that the `SearchIndexerEngineName` variable matches the type of Oracle UCM system to use (`DATABASE.METADATA`, `DATABASE.FULLTEXT`, or `OracleTextSearch`).
 - b. Under **Administration** tray, select **Admin Server**.
 - c. Click **idc**.
 - d. Select **General Configuration**, on the left.
 - e. Select **Automatically assign a content ID on check in**.
 - f. Specify an **Auto Number Prefix** value, such as `ucm1`.

- g. Set the `EnableIdcProfileField` variable to 1 by adding the following line to the Additional Configuration Variables box:

```
EnableIdcProfileField=1
```

- h. Click **Save**.

6. Install Oracle UCM components:

- a. Select **Component Manager**, on the left.
- b. In the Install New Component section, click **Browse**, 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 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 `ECM_ORACLE_HOME/ipm/lib` directory, and select **IpmRepository.zip**.
- i. Click **Open**.
- j. Click **Install**.

Restart Oracle Content Server 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 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 is running after you restart it.

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

To add the administrator user and Administrators group to Oracle UCM

1. In the Oracle UCM web client, select **Admin Applets** under **Administration**.
2. Click **User Admin**.
3. On the **Security** tab, select **Permissions By Role**.
4. Select **Add New Role**.
5. In the **Role Name** field, enter **Administrators**.
6. Click **OK**.
7. Click **Close**.
8. Click **Add**.
9. For **Authorization Type: Local**, click **OK**.
10. Create the administrator user, and enter the password.
11. Click the **Roles** tab.
12. Click **Add Role**.
13. Select **Administrators**, and then click **OK**.
14. Click **OK**.
15. Close the User Admin applet.

7.1.1.3 Configuring a File Store Provider for Content Storage

An administrator can configure a file store provider in Oracle Content Server 11g to control how and where files are stored and managed within the Oracle Content Server instance. 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 Oracle Content Server installation and configuration.

For Oracle I/PM, 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 Oracle Content Server 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 Oracle ECM installation uses a Microsoft SQL Server or IBM DB2 database, do not configure a file store provider. If you are configuring an Oracle UCM Managed Server with one of these databases, you need to disable the file store provider that is enabled by default for Oracle Content Server.

For more information, see "Configuring a File Store System" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Content Server*.

7.1.1.3.1 Configuring a File Store Provider A file store provider can be a combination of any media supported by Oracle 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 Oracle I/PM user

interface. Oracle I/PM connects to a volume defined and configured in Oracle Content Server by an administrator. You cannot use Oracle I/PM to create or define a volume.

An Oracle Content Server administrator can configure a file store provider. For more information, see "File Store Administration Interface" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Content Server*.

7.1.1.3.2 Disabling Web Layout Functionality for Oracle I/PM Oracle 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 Oracle I/PM solution. Files copied to a `/weblayout` directory in an exclusively Oracle I/PM 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 Oracle I/PM 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 Oracle Content Server. For more information, see "Add/Edit Storage Rule Page" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Content Server*.

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

After you start the Administration server and the Oracle I/PM and Oracle UCM Managed Servers, you can access the Oracle I/PM web client.

To access the Oracle I/PM web client:

1. Start the Oracle I/PM Managed Server, as described in [Section 10.2, "Starting Managed Servers."](#)
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 Oracle I/PM system is registered as the Oracle I/PM administrator.

7.1.3 Connecting to an Oracle UCM Repository

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

To connect to an Oracle UCM 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 Oracle UCM instance, 4444 for Oracle I/PM by default
 - **Use Local Content Server:** Selected by default if the Oracle UCM server is on the same machine as the Oracle I/PM server.

If the servers are not installed on the same machine, you will need to configure the Oracle UCM 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**.

7.1.4 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 Oracle I/PM 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, Oracle I/PM requires the GNU Compiler Collection (GCC) package 3.4.2 or later in the `/usr/local/packages` directory.

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

<http://www.sunfreeware.com>

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

- AIX: `/usr/lpp/X11/lib/X11/fonts/TrueType`
 - HP-UX Itanium: `/usr/lib/X11/fonts/TrueType`
9. Click **Apply**.
 10. Restart Oracle I/PM, as described in [Section 10.3, "Restarting a Managed Server."](#)

7.1.5 Allowing IMPORT Definitions

After you install Oracle Enterprise Content Management Suite and configure Oracle UCM and Oracle I/PM on Oracle WebLogic Server, you need to configure Oracle I/PM to allow IMPORT definitions.

To allow IMPORT definitions:

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, such as `UM11g`, on the Basic Information page, and optionally a description, and then click **Next**.
5. On the Connection Settings page, enter or change values as necessary, and click **Next**.
6. On the Review Settings page, if the settings are correct, click **Submit**.

After the connection is created, you should be able to use IMPORT definitions for your applications.

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

Oracle I/PM supports two types of full-text searching under Oracle UCM: DATABASE.FULLTEXT and Oracle Text Search. Oracle I/PM can use the full-text features if you configure full-text searching in the Oracle UCM repository first. For DATABASE.FULLTEXT systems, after the indexes are rebuilt, nothing needs to be done on the Oracle I/PM side. Oracle Text Search, 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 5.3, "Configuring Oracle Text Search for Oracle Content Server."](#)

For additional full-text configuration options, see "Configuring the Search Index" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Content Server*.

After full-text is enabled in Oracle UCM, you will need to create an application and check the FullText option on the application. For more information, see "Specifying General Properties" in *Oracle Fusion Middleware Administrator's Guide for Oracle Imaging and Process Management*.

7.3 Connecting to a Workflow Server

A connection to a workflow server will be necessary for your solution to retrieve your task list. Oracle I/PM 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. Oracle I/PM 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 Oracle I/PM 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 Fusion Middleware Administrator's Guide for Oracle Imaging and Process Management*.

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**.

7.4 Setting Oracle I/PM System Security

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

Note: If you configure Oracle I/PM for use with Oracle Access Manager, you must protect the `imaging/faces/` directory. Failure to do so would prevent access to the Oracle I/PM Viewer.

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

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

For more information, see [Section 4.9, "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 Oracle I/PM database.

7.5 Installing and Configuring Oracle Application Extension Framework

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

For Oracle Application Extension Framework (AXF) to work with Oracle I/PM 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.

7.5.1 Configuring the Java Object Cache for AXF in Distributed Oracle I/PM Managed Servers

You can use the `MW_HOME/oracle_common/bin/configure-joc.py` Python script, in the Middleware home, to configure the JOC on all of the Managed Servers in distributed mode. The script runs in the Oracle WebLogic Scripting Tool (WLST) online mode and expects the Administration Server to be up and running.

Note: After configuring the Java Object Cache, restart all affected Managed Servers for the configurations to take effect, as described in [Section 10.3, "Restarting a Managed Server."](#)

To enable the JOC in distributed mode with the configure-joc.py script:

1. Connect to the Administration Server with a WLST command; for example:

```
MW_HOME/oracle_common/common/bin/wlst.sh
$ connect()
```

Enter the Oracle WebLogic Server Administration user name and password when prompted.

2. After connecting to the Administration Server with WLST, use the `execfile` command to start the script; for example:

```
wls:/mydomain/serverConfig>execfile('MW_HOME/oracle_
common/bin/configure-joc.py')
```

3. Configure JOC for all the managed servers for a given cluster.

Enter `y` when the script prompts whether you want to specify a cluster name, and also specify the cluster name and discover port when prompted. This discovers all the Managed Servers for the given cluster and configures the JOC for each Managed Server. The discover port is common for the entire JOC configuration across the cluster. An example follows:

```
Do you want to specify a cluster name (y/n) <y> y
Enter Cluster Name : IPM_Cluster
Enter Discover Port : 9988
```

Here is a sample walkthrough for using `configure-joc.py` for clustered environments:

```
execfile('MW_HOME/oracle_common/bin/configure-joc.py')
.
Enter Hostnames (eg host1,host2) : IPMHOST1, IPMHOST2
.
Do you want to specify a cluster name (y/n) <y> y
.
Enter Cluster Name : IPM_Cluster
.
Enter Discover Port : 9991
.
Enter Distribute Mode (true|false) <true> : true
.
Do you want to exclude any server(s) from JOC configuration (y/n) <n> n
```

For more information, see "Configuring the Distributed Java Object Cache" in *Oracle Fusion Middleware High Availability Guide*.

7.5.2 Verifying the AXF Installation with HelloWorld

Follow these steps to enable the HelloWorld solution:

1. As user who owns the Oracle I/PM schema, run the `insertHelloCommand.sql` script from the following directory:
 - **UNIX path:**
`MW_HOME/ECM_ORACLE_HOME/axf/drivers/HelloWorld/dbscripts`
 - **Windows path:**
`MW_HOME\ECM_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.

7.5.3 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/ECM_ORACLE_HOME/axf/drivers/HelloBpel`
- **Windows path:**
`MW_HOME\ECM_ORACLE_HOME\axf\drivers\HelloBpel`

To enable the HelloBpel solution:

1. Run one of the following `HelloBPEL` SQL scripts:

- **UNIX scripts:**

```
MW_HOME/ECM_ORACLE_HOME/axf/drivers/HelloBpel/dbscripts
/oracle/insertHelloBPELData.sql
```

```
MW_HOME/ECM_ORACLE_HOME/axf/drivers/HelloBpel/dbscripts
/sqlserver-db2/insertHelloBPELData.sql
```

- **Windows scripts:**

```
MW_HOME\ECM_ORACLE_HOME\axf\drivers\HelloBpel\dbscripts
\oracle\insertHelloBPELData.sql
```

```
MW_HOME\ECM_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 11g, open `HelloBPEL.jws` from following directory:

- **UNIX path:**

```
MW_HOME/ECM_ORACLE_HOME/axf/drivers/HelloBpel/bpel
```

- **Windows path:**

```
MW_HOME\ECM_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 Oracle I/PM user; for example, `weblogic`

The preceding Oracle I/PM 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.

7.6 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 *Oracle Document Capture Installation Guide* and *Oracle Document Capture Administrator's Guide*.

For information about installing and configuring Oracle Distributed Document Capture, see *Oracle Distributed Document Capture Installation Guide* and *Oracle Distributed Document Capture Administrator's Guide*.

The Oracle I/PM 11g Commit Driver is required to commit documents from either capture application to Oracle UCM. For information about using the Oracle I/PM 11g Commit Driver, see *Oracle Distributed Document Capture Installation Guide* or *Oracle Distributed Document Capture Administrator's Guide*.

Configuring Oracle Information Rights Management

This chapter explains how to configure an Oracle Information Rights Management (Oracle IRM) application in an Oracle WebLogic Server domain, in these topics:

- [Performing Postinstallation Configuration](#)
- [Validating the Oracle IRM Installation](#)
- [Configuring the Identity Store](#)
- [Integrating Oracle IRM with Oracle Access Manager 11g](#)

8.1 Performing Postinstallation Configuration

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

- [Setting the Server URL Configuration Parameter for Oracle IRM](#)
- [Configuring a Key Store for Oracle IRM](#)

Note: In a production environment, Oracle Enterprise Content Management Suite (Oracle ECM) 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 4.9, "Reassociating the Identity Store with an External LDAP Authentication Provider."](#)

8.1.1 Setting the Server URL Configuration Parameter for Oracle IRM

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

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

For a simple installation where the Managed Server is directly accessible to Oracle IRM Desktop, this value will be the URL of the 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 **Content Management** and **Information Rights Management**, and then click **IRM**.
3. From the **IRM** menu, select **Administration** and then **General Settings**.
Fusion Middleware Control displays the General Settings page.
4. In the **Server URL** field, enter the URL to access the Oracle IRM Managed Server.
For a simple installation where the Managed Server is directly accessible to Oracle IRM Desktop, this value will be the URL of the 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**.

8.1.2 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](#)

8.1.2.1 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.

8.1.2.1.1 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>

8.1.2.1.2 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.

8.1.2.2 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 an 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`

8.1.2.3 Setting the Key Store Location

The Oracle IRM 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 ECM 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 **Content Management** and **Information Rights Management**, 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**

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

– **Windows operating system**

```
ECM_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

8.1.2.4 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 Oracle IRM server.

To add key store passwords to the credential store:

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

– **UNIX operating system**

```
ECM_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**

```
ECM_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**

```
ECM_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**

```
ECM_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.
-
-

8.1.2.5 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 4.9, "Reassociating the Identity Store with an External LDAP Authentication Provider."](#)

8.2 Validating the Oracle IRM Installation

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 installation was successful by accessing this URL:

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

For example:

```
https://myhost.example.com:16101/irm_desktop
```

8.3 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 4.9, "Reassociating the Identity Store with an External LDAP Authentication Provider."](#)

8.4 Integrating Oracle IRM with Oracle Access Manager 11g

Oracle Access Manager is the recommended single sign-on (SSO) solution for Oracle Enterprise Content Management Suite 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/.../*

IRM 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 Oracle IRM 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. Oracle IRM 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:

- Oracle IRM Desktop is supported only with Oracle Access Manager 10g and not with Oracle Access Manager 11g for Release 11.1.1.4.0.
- For information about Oracle Access Manager 10g, 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 11g, you can configure it and Oracle IRM to work together.

Note: The following procedure should be performed only after you have installed Oracle Enterprise Content Management Suite (described in [Chapter 3, "Installing Oracle Enterprise Content Management Suite"](#)) and configured an Oracle IRM Managed Server (described in [Chapter 4, "Configuring Oracle Enterprise Content Management Suite"](#)). 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 11g, 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 11g, 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 ECM 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 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*, 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 ECM 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 11g, 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`.

Configuring Oracle Universal Records Management

This chapter explains how to configure Oracle Universal Records Management (Oracle URM) in an Oracle WebLogic Server domain, in these topics:

- [Completing the Oracle URM Configuration](#)
- [Using Oracle Text Search with Oracle URM](#)
- [Setting Connection Pool Property Values for an IBM DB2 Data Source](#)
- [Installing and Configuring Desktop Integration Suite on a Client Workstation](#)

9.1 Completing the Oracle URM Configuration

After installation and startup, when you go to the URL for Oracle URM, you will get the postinstallation configuration page, described in [Section 9.1.1, "Enabling Oracle URM Components."](#) After completing that page and clicking the **Submit** button, you need to restart Oracle URM, as described in [Section 10.3, "Restarting a Managed Server."](#) It is installed with default installation level of minimal.

Oracle URM will start up again with an alert. Clicking the alert text displays the Records Management Setup Checklist, through which you can configure the Oracle URM installation level you want. For more information about setting the installation level, see [Section 9.1.1, "Enabling Oracle URM Components."](#) If you change the installation level, you need to restart the Oracle URM Managed Server and rebuild the index. For information about rebuilding the index, see "Working with the Search Index" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Content Server*.

After you configure the installation level, you can configure other items on the Setup Checklist page. For more information, see [Section 9.1.2, "Completing the Setup Checklist for Oracle URM."](#)

9.1.1 Enabling Oracle URM Components

The Enabled Features Page determines which Oracle URM components will be enabled for use.

Records Management Installation Configuration

Select a preset configuration below, or use the Custom option to choose your own settings. Note that you will need to restart the server after making any changes here.

Installation levels

- Minimal (i)
- Typical (i)
- DoD Baseline (i)
- DoD Classified (i)
- Custom (i)

Features

<input checked="" type="checkbox"/> Related Content	<input checked="" type="checkbox"/> Audit Trigger	<input checked="" type="checkbox"/> Subject to Review
<input checked="" type="checkbox"/> Revision Dates	<input checked="" type="checkbox"/> Security Markings	<input checked="" type="checkbox"/> Email Fields
<input checked="" type="checkbox"/> DoD Configuration	<input type="checkbox"/> Classified Topics	<input type="checkbox"/> FOIA-Privacy Act

Disposition Actions

<input checked="" type="checkbox"/> Activate	<input checked="" type="checkbox"/> Obsolete	<input checked="" type="checkbox"/> Cancel
<input checked="" type="checkbox"/> Rescind	<input checked="" type="checkbox"/> Expire	<input checked="" type="checkbox"/> Cutoff
<input checked="" type="checkbox"/> Approve Deletion	<input checked="" type="checkbox"/> Destroy	

The page depiction shows all options displayed.

Note: If you are using Oracle WebCenter with Oracle URM, enable the DOD component after WebCenterConfigure has been enabled and has had a chance to check in its conversion templates.

If you enable the DOD component first, you can create a rule that matches the documents created by WebCenterConfigure and assigns them a default category. The category could be based on the content IDs. For more information, see "Setting Up Workflows" in *Oracle Fusion Middleware Setup Guide for Universal Records Management*.

After making selections or if configuration options are changed (for example, switching from **Baseline** to **Classified**), restart Oracle Universal Records Management, as described in [Section 10.3, "Restarting a Managed Server,"](#) and rebuild the Oracle Content Server index. For information about rebuilding the index, see "Working with the Search Index" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Content Server*.

For information about the components enabled for each option, click the **Info** icon.

Element	Description
Installation Level	<p>The type of configuration to be enabled. Options are:</p> <ul style="list-style-type: none"> ■ Minimal ■ Typical ■ DoD Baseline ■ DoD Classified ■ Custom
Features	<p>This section contains a list of features that can be enabled when using the Custom option. Default features are enabled when installation levels are chosen.</p> <p>These features include:</p> <ul style="list-style-type: none"> ■ Related Content ■ Audit Trigger ■ Subject to Review ■ Revision Dates ■ Security Markings ■ Email Fields ■ DoD Configuration ■ Classified Topics ■ FOIA/Privacy Act
Disposition Actions	<p>This section contains the disposition actions which can be used for content. They include:</p> <ul style="list-style-type: none"> ■ Activate ■ Rescind ■ Approve Deletion ■ Obsolete ■ Expire ■ Destroy ■ Cancel ■ Cutoff

9.1.2 Completing the Setup Checklist for Oracle URM

After the installation and configuration of Oracle URM on an Oracle WebLogic Server 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 Fusion Middleware Setup Guide for Universal Records Management*.

Figure 9–1 Oracle URM Setup Checklist

Records Management Setup Checklist

Use this page as a reminder of items that must be set up before using your system. Use the active links below or choose these options from the main Records menu. Use the check boxes to mark items that have been completed.

Detailed documentation is available for each option. Click the Quick Help button then navigate to the appropriate chapter for more information.

[Expand All Details](#)

- ▶
[Configure Installation](#)
✓

- ▶
Define Defaults : (refresh the page once the action is executed)
 - [Install Data Resource Files \(Schema etc.\)](#) Done
 - [Install Default Templates \(Category Defaults, Reports , Dashboards etc.\)](#) Done
 - [Checked-in Audit Entries Default Metadata](#) Done
 - [Checked-in Screening Reports Default Metadata](#) Done
 - [Checked-in Reservation Default Metadata](#) Done
 - [Checked-in Offsite Default Metadata](#) Done

- ▶
[Configure Security Settings \(User Admin Applet\)](#)
✓

- ▶
[Configure Retention Management Settings](#)
✓

- ▶
[Configure Fiscal, Calendar, and Custom Periods](#)
✓

- ▶
[Configure Global, Direct, and Indirect Triggers](#)
✓

- ▶
[Create Retention Schedule](#) or [Import Retention Schedule](#)
✓

- ▶
[Configure Freeze Reasons](#)
✓

- ▶
[Configure Workflows \(Workflow Admin Applet\)](#)
✓

- ▶
[Configure Default Reviewers \(User Admin Applet\)](#)
✓

- ▶
[Configure Related Content Types](#)
✓

- ▶
Configure 'Profile Trigger' as Trigger Field for:
 - [Content](#) Done
 - [Retention Categories](#) Done
 - [Records Folders](#) Done
 - [Physical](#) Done

If the configuration tasks on this page are not completed, a warning message with a link to this page appears on the home page of the Oracle Content Server system. Click the link to display this page.

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.

Selecting any option in this list displays a detailed explanation of the option's purpose. The options available on the page depend on your installation level:

- Minimal
- Typical
- DoD Baseline
- DoD Classified
- Custom

Element	Description
Configure Installation	Used to configure optional components and metadata fields. Select from preset configurations to choose the features that are needed.
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 <i>Oracle Fusion Middleware Setup Guide for Universal Records Management</i> .
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 <i>Oracle Fusion Middleware Setup Guide for Universal Records Management</i> .
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 <i>Oracle Fusion Middleware Setup Guide for Universal Records Management</i> .
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 <i>Oracle Fusion Middleware Administrator's Guide for Universal Records Manager</i> . For information about this page, see "Exploring Retention Schedule Page" in <i>Oracle Fusion Middleware Setup Guide for Universal Records Management</i> .

Element	Description
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 <i>Oracle Fusion Middleware Setup Guide for Universal Records Management</i> .
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 <i>Oracle Fusion Middleware Setup Guide for Universal Records Management</i> .
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 <i>Oracle Fusion Middleware User's Guide for Universal Records Manager</i> .
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: <ul style="list-style-type: none"> ■ 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.

9.2 Using Oracle Text Search with Oracle URM

When you use Oracle Text Search with Oracle Content Server, 32 optimized fields are allowed. When Oracle URM is installed, the number of optimized fields can exceed the 32-field limit.

To accommodate this limitation, if Oracle Text Search is configured as the search engine, Oracle URM sets its date fields to be nonsearchable. Because of this, Oracle URM date fields will not appear on search pages.

If you installed Oracle URM while using Oracle Text Search and later change search engines, you can configure the date fields to be searchable by using the Oracle Content Server Configuration Manager.

If you install URM without Oracle Text Search and later change your current search engine to Oracle Text Search, you must manually configure the date fields to be nonsearchable in the Oracle Content Server Configuration Manager.

To search auxiliary metadata in Oracle URM with Oracle Text, you must configure Oracle Content Server to use Oracle Text Search as the search engine. You can set Oracle Text Search on the Oracle UCM postinstallation configuration page or in the configuration file. For more information, see [Section 5.3, "Configuring Oracle Text Search for Oracle Content Server."](#)

9.3 Setting Connection Pool Property Values for an IBM DB2 Data Source

If the Oracle URM 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 Oracle URM 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.

9.4 Installing and Configuring Desktop Integration Suite on a Client Workstation

The Desktop Integration Suite component provides a set of embedded applications that help you seamlessly integrate your desktop experience with Oracle Content Server. More specifically, it provides convenient access to Oracle 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 install the Desktop Integration Suite on a client workstation, see "Setting Up Desktop Integration on Client Computers" in *Oracle Fusion Middleware User's Guide for Desktop Integration Suite*.

Verifying the Installation and Configuration

This chapter explains how to verify successful installation and complete the configuration of Oracle Enterprise Content Management Suite applications, in these topics:

- [Starting the Administration Server](#)
- [Starting Managed Servers](#)
- [Starting Node Manager](#)
- [Increasing the Java Heap Size for a Managed Server](#)
- [Verifying the Installation](#)

10.1 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 Oracle UCM Managed Server as an administrator before you can access Oracle Content Server through the web interface for Oracle UCM.

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.

10.2 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 Oracle I/PM Managed Server and logging in for the first time, see [Section 7.1, "Completing the Oracle I/PM Configuration,"](#) and do not start the Managed Server until you have completed the tasks before [Section 7.1.2, "Starting the Oracle I/PM Managed Server and Accessing the Web Client."](#)
- Before logging in to the Oracle IRM Management Console for the first time or using Oracle IRM Desktop, see [Section 8.1, "Performing Postinstallation Configuration."](#)
- On a Windows operating system that has User Account Control (UAC) enabled, you need to start the Oracle WebLogic Server Administration Server and Oracle UCM Managed Server as an administrator before you can access Oracle Content Server through the web interface for Oracle UCM.

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 Oracle UCM Managed Server, as described in the following procedure. For information about accessing Oracle Content Server, see [Section 10.6, "Verifying the Installation."](#)

To start a Managed Server:

1. Start the Administration Server (see [Section 10.1, "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` (Oracle Universal Content Management)
- `IBR_server1` (Oracle Inbound Refinery)
- `IPM_server1` (Oracle Imaging and Process Management)
- `IRM_server1` (Oracle Information Rights Management)
- `URM_server1` (Oracle Universal Records Management)

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/`.

For example, the following script would start an Oracle I/PM 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 an Oracle IRM Managed Server on the local host:

```
MW_HOME\user_projects\domains\domain_name\bin\  
startManagedWebLogic.cmd IRM_server1
```

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

The 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
```

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*.

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.

10.3 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 Fusion Middleware System Administrator's Guide for Oracle 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

10.4 Starting Node Manager

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

Before you start Node Manager, be sure to complete the Oracle URM setup checklist, described in [Section 9.1, "Completing the Oracle URM Configuration."](#)

To start Node Manager:

1. Start Node Manager with the `startNodeManager` script.

UNIX script: *WL_HOME/server/bin/startNodeManager.sh*

Windows script: *WL_HOME\server\bin\startNodeManager.cmd*

2. Edit the `nodemanager.properties` file to change the entry `StartScriptEnabled=false` to `StartScriptEnabled=true`.
3. Restart Node Manager.

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 Oracle UCM Managed Server as an administrator before you can access Oracle Content Server through the web interface for Oracle UCM. If you want to use Node Manager to start the Oracle UCM 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.
 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, as described in [Section 10.1, "Starting the Administration Server."](#)
 5. Open another Command Prompt window with the **Run As Administrator** option.
 6. Start Node Manager in it, as described in the preceding procedure.
 7. Access the Oracle WebLogic Server Administration Console, as described in [Section 10.6, "Verifying the Installation,"](#) click **Servers**, and start the Oracle UCM Managed Server.
-

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

10.5 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 ECM 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 10.3, "Restarting a Managed Server."](#)

10.6 Verifying the Installation

To verify the installation of Oracle Enterprise Content Management Suite, start a web browser, and enter the following URLs to test access to the 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 Enterprise Management Suite applications.

- To test a newly set up Oracle UCM instance by accessing Oracle Content Server:

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

Log in with the user name and password for Oracle WebLogic Server. The default port number for Oracle UCM is 16200.

- To test a newly set up Oracle IBR instance:

```
http://managedServerHost:managedServerPort/ibr
```

Log in with the user name and password for Oracle WebLogic Server. The default port number for Oracle IBR is 16250.

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

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

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

- To test a newly set up Oracle IRM instance:

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

- To test a newly set up Oracle URM instance:

```
http://managedServerHost:managedServerPort/urm
```

Log in with the user name and password for Oracle WebLogic Server. The default port number for Oracle URM is 16300.

Deinstalling Oracle Enterprise Content Management Suite

This chapter explains how to deinstall Oracle Enterprise Content Management Suite, in these topics:

- [Introduction to Deinstalling Oracle Enterprise Content Management Suite](#)
- [Stopping Oracle WebLogic Server and Server Processes](#)
- [Removing Oracle Enterprise Content Management Suite Schemas](#)
- [Deinstalling the ECM Oracle Home](#)
- [Removing Oracle Home Directories Manually](#)

11.1 Introduction to Deinstalling Oracle Enterprise Content Management Suite

Deinstalling Oracle Enterprise Content Management Suite 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.

11.2 Stopping Oracle WebLogic Server and Server Processes

Before deinstalling the Oracle Enterprise Content Management Suite component of Oracle Fusion Middleware, you should stop all servers and processes.

1. Stop each Managed Server in the Oracle WebLogic Server domain with the `stopManagedWebLogic` script in the *DomainHome/bin* directory.
 - **UNIX script:** `MW_HOME/user_projects/domains/DomainHome/bin/stopManagedWebLogic.sh managed_server_name admin_url username password`

For example:

```
/middleware_home/user_projects/domains/ecm_domain/bin/  
stopManagedWebLogic.sh IPM_server1 myhost.oracle.com:16000  
weblogic password
```

- **Windows script:** `MW_HOME\user_projects\domains\DomainHome\bin\stopManagedWebLogic.cmd managed_server_name admin_url username password`
- 2. Stop the Administration Server:
 - **UNIX operating system**
`MW_HOME/user_projects/domains/domain_name/bin/stopWeblogic.sh
username password`
 - **Windows operating system**
`MW_HOME\user_projects\domains\domain_name\bin\stopWeblogic.cmd
username password`

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

11.3 Removing Oracle Enterprise Content Management Suite Schemas

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

11.3.1 Starting Repository Creation Utility

Insert the Repository Creation Utility DVD, 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 also download a ZIP file containing the Repository Creation Utility from either of these web sites:

- Oracle E-Delivery at
<http://edelivery.oracle.com/>
- Oracle Fusion Middleware 11g 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.

11.3.2 Dropping Schemas

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

1. Welcome screen

Click **Next**.

2. Create Repository screen

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

3. Database Connection Details screen

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

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

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

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

4. Select Components screen

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

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

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

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

5. Summary screen

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

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

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

After the schemas are dropped with no errors, click **OK** to dismiss the screen.

6. Completion Summary screen

Click **Close**.

11.4 Deinstalling the ECM Oracle Home

The deinstaller attempts to remove the ECM Oracle home from which it was started. Before you remove the Oracle home for Oracle Enterprise Content Management Suite, make sure that it is not in use by an existing domain and that you stop all running processes that use this Oracle home. After you remove the software, you will no longer be able to use your 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 ECM Oracle home.

Follow the instructions in [Table 11–1](#) to deinstall Oracle Enterprise Content Management Suite. The procedure after the table describes these steps in more detail.

Note: The deinstaller will attempt to remove the Oracle home directory from which it was started. Before you choose to remove the Oracle home, make sure that it is not in use by an existing domain.

Table 11–1 Deinstallation Procedure

No.	Screen	Description and Action Required
1	None	<p>Start the Oracle ECM installer with the <code>-deinstall</code> option from the <code>bin</code> subdirectory of the <code>oui</code> directory in your ECM Oracle home:</p> <ul style="list-style-type: none"> ▪ UNIX command: <code>ECM_ORACLE_HOME/oui/bin/runInstaller -deinstall -jreLoc jre_location</code> ▪ Windows command: <code>ECM_ORACLE_HOME\oui\bin\setup.exe -deinstall -jreLoc jre_location</code> <p>If you double-click <code>setup.exe</code>, you will be prompted for the JRE location. After you enter the path, click Enter to start the installer.</p> <p>The value of <code>jre_location</code> must specify the absolute path to the Java Runtime Environment (JRE) on your system. A relative path will not work. For more information about the JRE location, see Section 3.2.5, "Installing Oracle Enterprise Content Management Suite."</p> <p>You can also start the installer from <code>Disk 1</code> of the Oracle Enterprise Content Management Suite media.</p> <p>On a Windows operating system, you can also start the installer from the Start menu by selecting Programs, then Oracle ECM 11g - Home1, and then Uninstall.</p>
2	Welcome	Click Next to continue.
3	Deinstall Oracle Home	<p>Verify the Oracle home you are about to deinstall.</p> <p>Click Deinstall to continue.</p>
4	Deinstallation Progress	<p>This screen shows the progress and status of the deinstallation.</p> <p>No action is necessary on this screen.</p>
5	Deinstallation Complete	Click Finish to dismiss the screen.

11.5 Removing Oracle Home Directories Manually

If the deinstallation procedure did not remove your ECM Oracle home directory, you need to manually remove it and all of its subdirectories.

To remove an ECM Oracle home directory on a UNIX operating system:

1. Change directories to the directory that contains the ECM Oracle home directory:

```
cd MW_HOME
```

2. Specify the name of the ECM Oracle home directory in this command:

```
rm -rf ECM_ORACLE_HOME
```

To remove an ECM Oracle home directory on a Windows operating system:

- In Windows Explorer, you can navigate to the `C:\MW_HOME` directory, right-click the `ECM_ORACLE_HOME` folder, and then choose **Delete** from the **File** menu.
- Alternatively, 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**

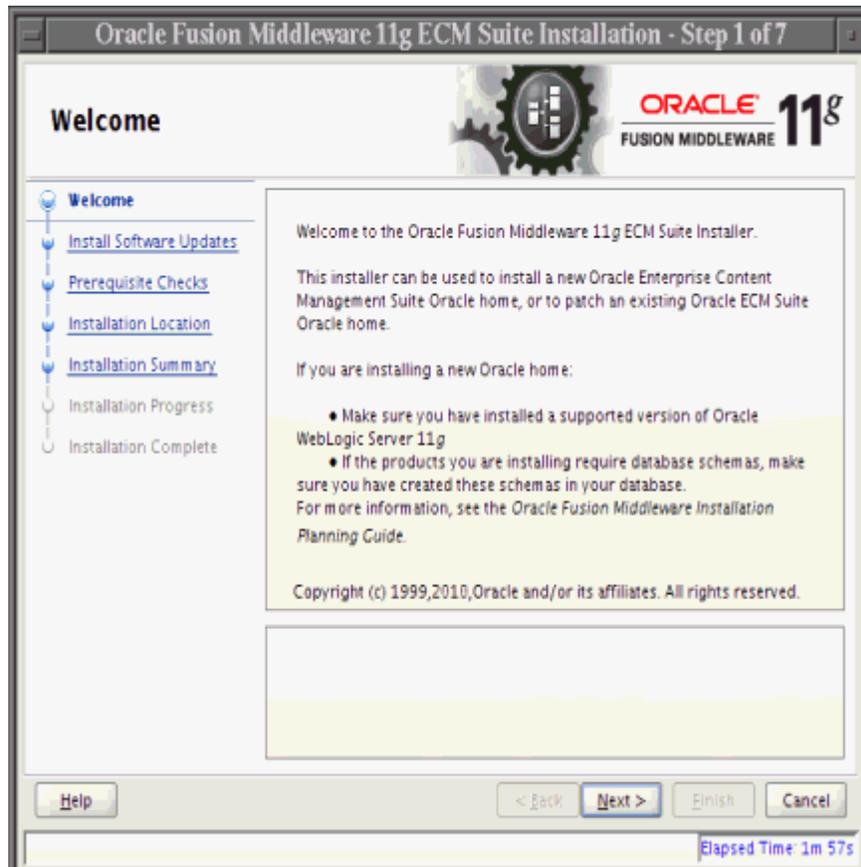
The folder and program group names on your Windows operating system might be different.

Oracle Enterprise Content Management Suite Installation Screens

This appendix describes Oracle Fusion Middleware 11g ECM Suite Installation screens for installing the Oracle Enterprise Content Management Suite component of Oracle Fusion Middleware:

- [Welcome](#)
- [Install Software Updates](#)
- [Prerequisite Checks](#)
- [Specify Installation Location](#)
- [Installation Summary](#)
- [Installation Progress](#)
- [Installation Completed](#)

A.1 Welcome



Each time the installer starts, it displays the Welcome screen.

The **Next** button continues the installation.

The **Cancel** button stops the installation.

A.2 Install Software Updates



This screen enables you to search for and install software updates before you install Oracle Enterprise Content Management Suite. 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**.

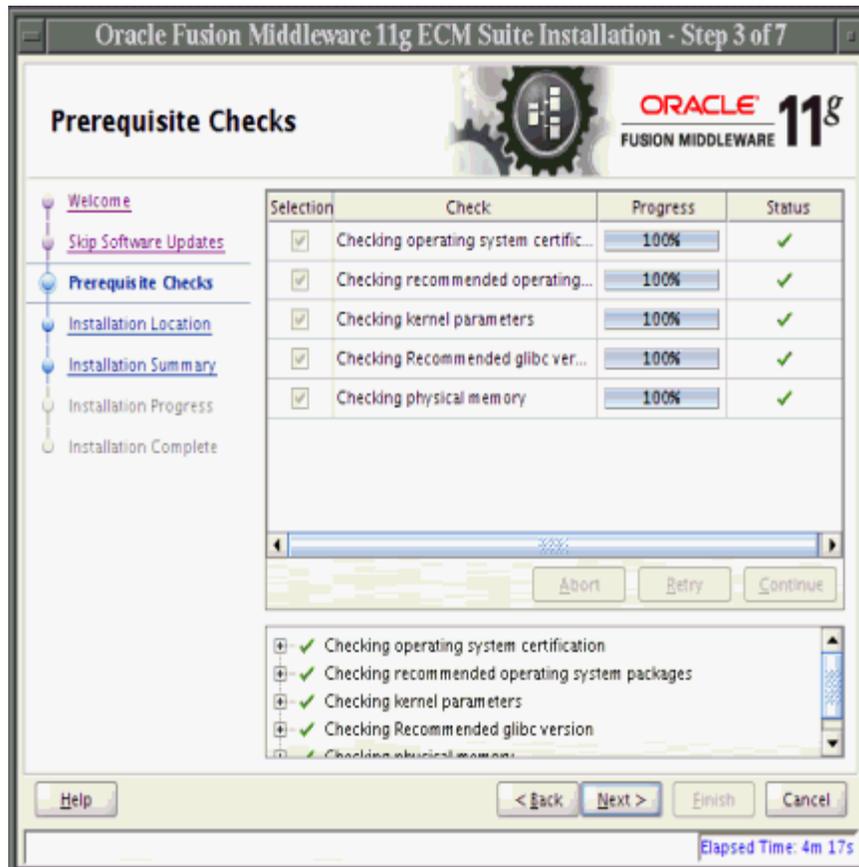
If you do not want to update any software, you can select **Skip Software Updates**. The link on the left changes from **My Oracle Support Updates** to **Skip Software Updates**.

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 UNIX operating system. Only three checks are performed for a Windows operating system:

- Checking operating system certification
- Checking Service Pack
- Checking physical memory

The installer displays any error or warning messages in the bottom section of the screen.

The **Abort** button stops prerequisite checking for all applications.

The **Retry** button starts prerequisite checking again for all applications.

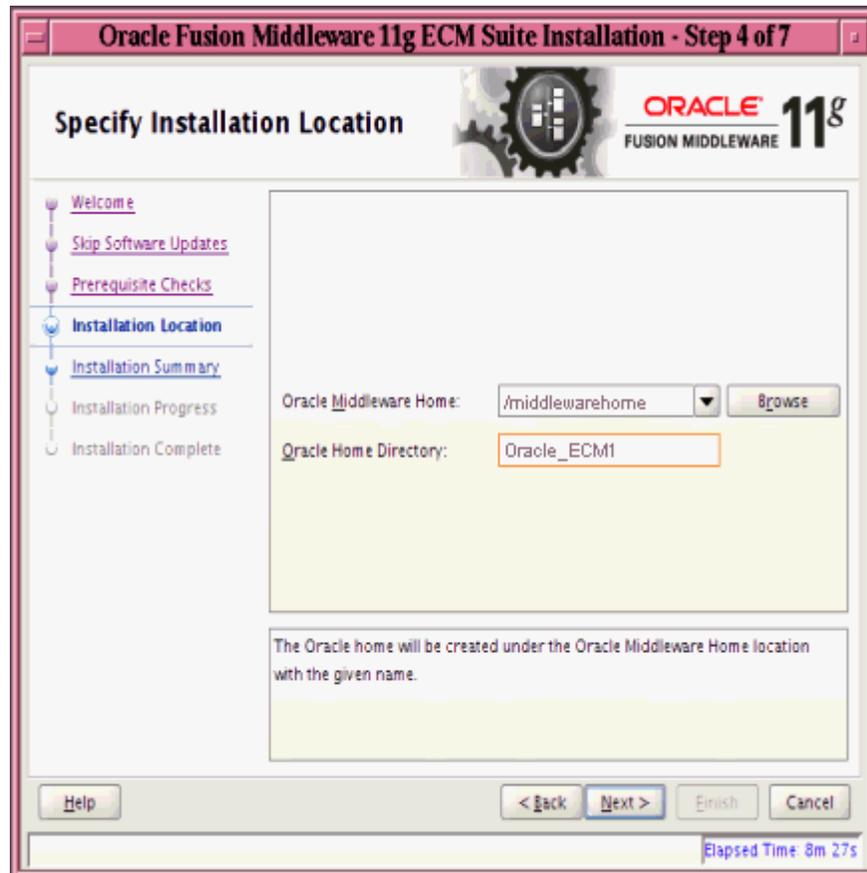
The **Continue** button continues the installation even if the screen displays an error or warning message.

The **Back** button returns to the 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, inside the Middleware home directory, in which to install Oracle Enterprise Content Management Suite (the ECM Oracle home directory). This directory must be empty. If the directory does not exist, the installer creates it.

The ECM Oracle home directory is where all Oracle Enterprise Management Content Suite products will be installed. All software binaries will reside in this directory, and no runtime process can write to this directory.

The **Back** button returns to the previous screen.

The **Next** button continues the installation after the prerequisite check completes with no errors.

The **Cancel** button stops the installation.

A.5 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.

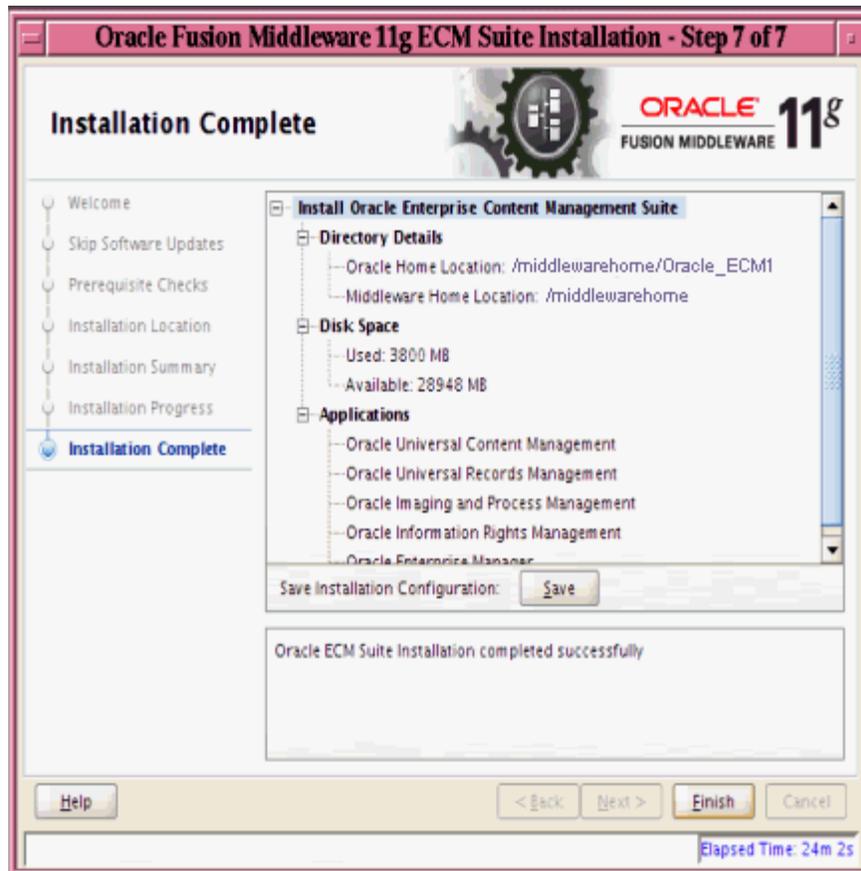
A.6 Installation Progress



This screen shows you the percentage of progress for the installation.

The **Cancel** button stops the installation before it completes.

A.7 Installation Completed



This screen indicates that the installation of Oracle Enterprise Content Management Suite is complete and summarizes its configuration.

The **Save** button saves the installation configuration in a file, which you can use later to perform the same installation from the command line.

The **Finish** button exits the configuration wizard.

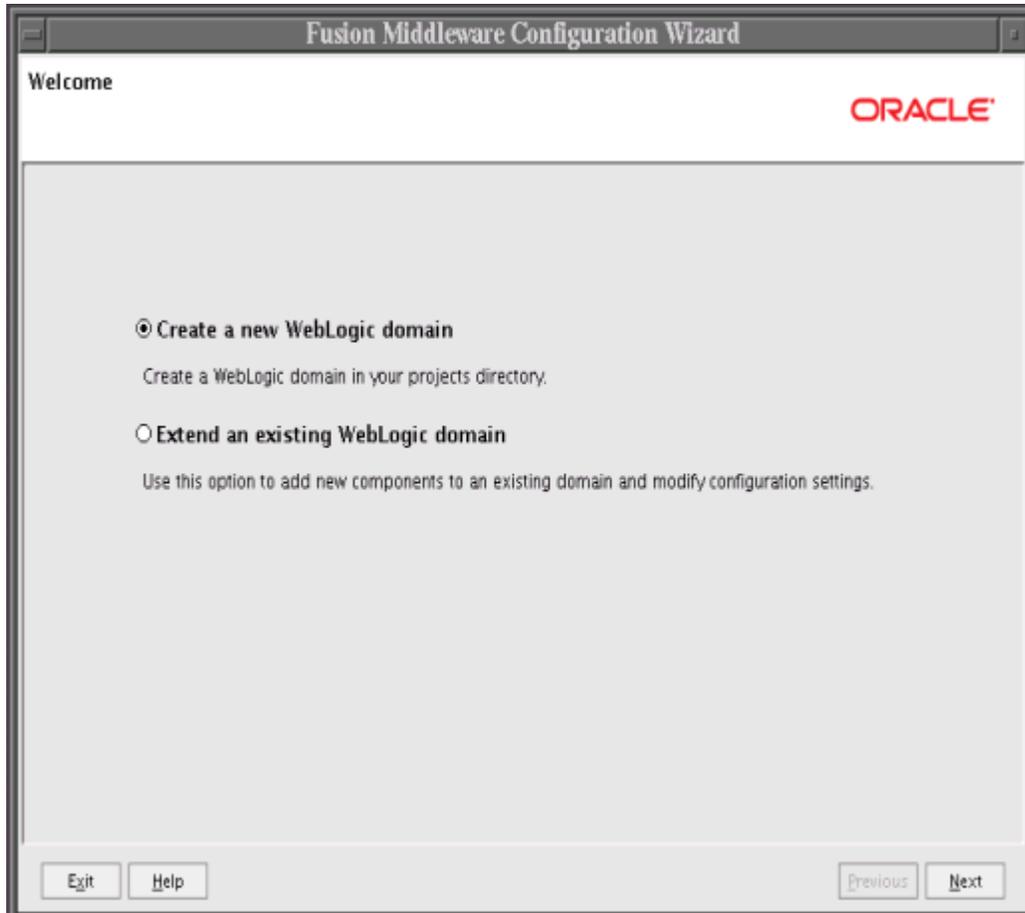
Oracle Enterprise Content Management Suite Configuration Screens

This appendix describes Fusion Middleware Configuration Wizard screens for configuring Oracle Enterprise Content Management Suite applications:

- Welcome
- Select a WebLogic Domain Directory
- Select Domain Source
- Select Extension Source
- Specify Domain Name and Location
- Configure Administrator User Name and Password
- Configure Server Start Mode and JDK
- Configure JDBC Component Schema
- Test Component Schema
- Select Optional Configuration
- Configure the Administration Server
- Configure Managed Servers
- Configure Clusters
- Assign Servers to Clusters
- Create HTTP Proxy Applications
- Configure Machines
- Assign Servers to Machines
- Target Deployments to Clusters or Servers
- Target Services to Clusters or Servers
- Select JMS Distributed Destination Type
- Configure RDBMS Security Store Database
- Configure JMS File Stores
- Configuration Summary
- Creating Domain
- Extending Domain

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 Welcome



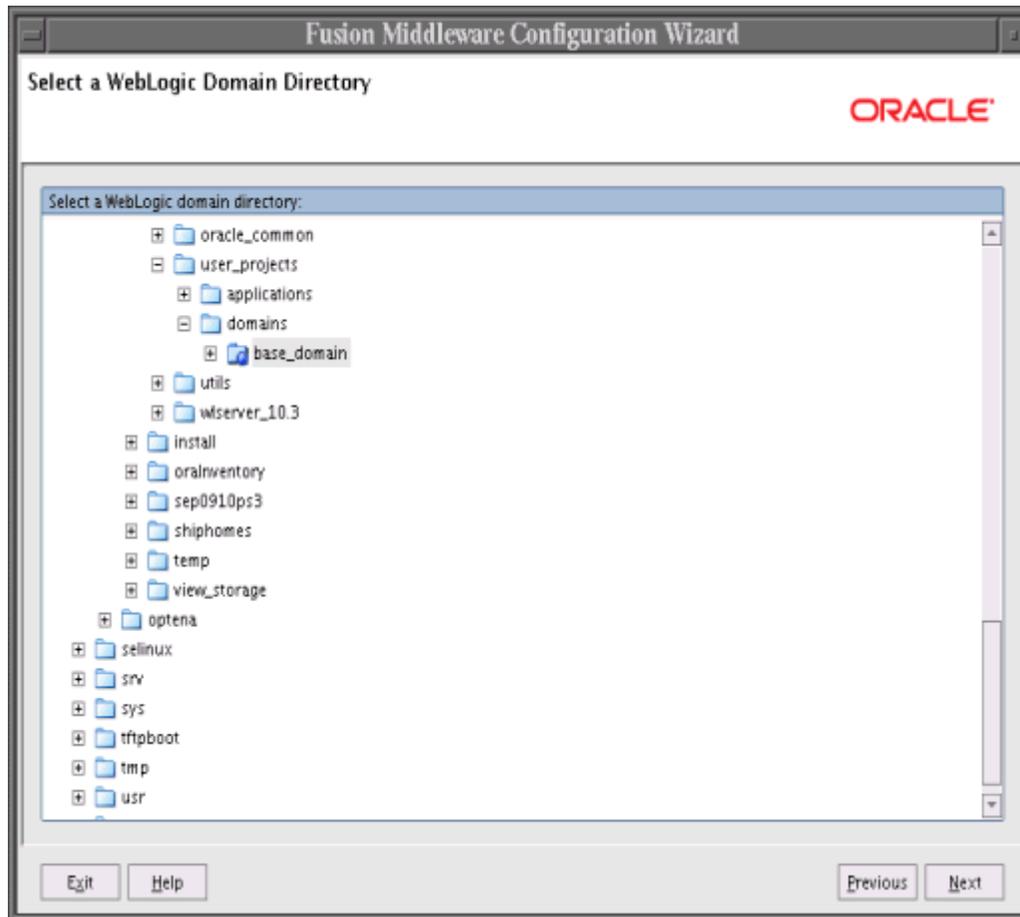
The Welcome screen appears each time you start the configuration wizard.

Select **Create a new WebLogic domain** to create a new Oracle WebLogic Server domain in your `projects` directory.

Select **Extend an existing WebLogic domain** if you want to add applications and services, or to override existing database access (JDBC) and messaging (JMS) settings.

Click **Next** to continue.

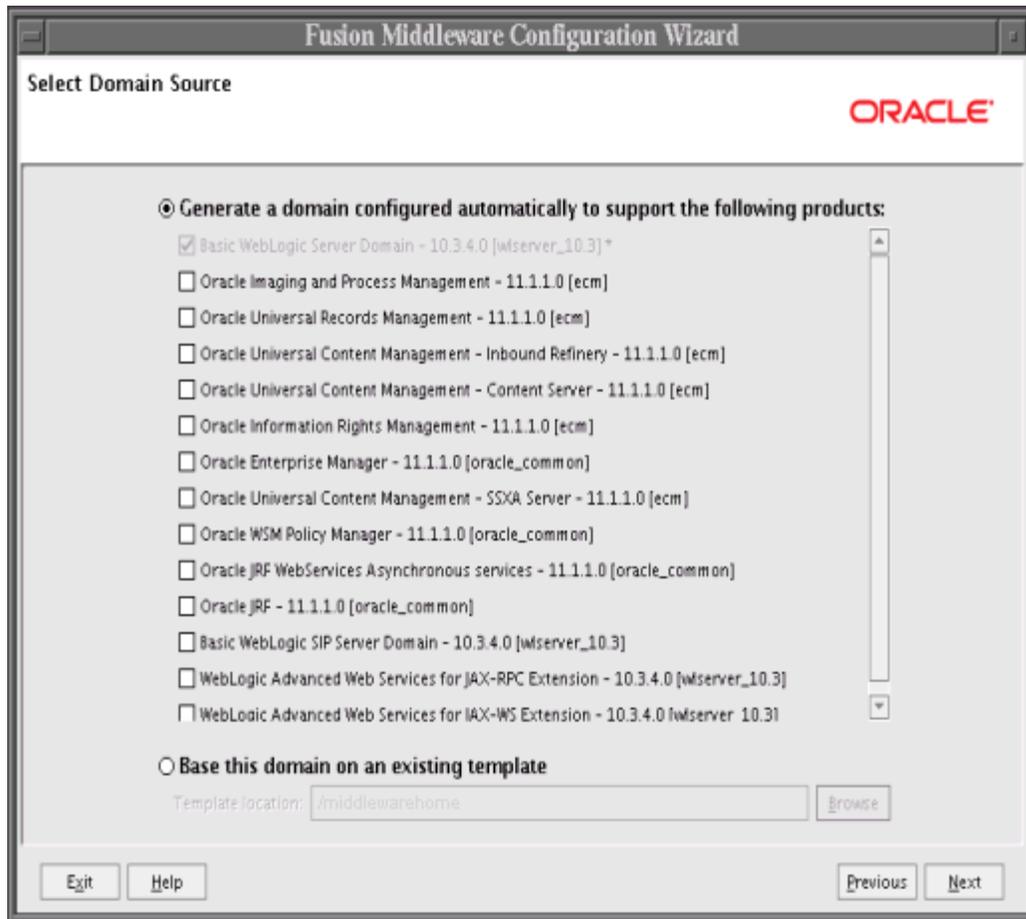
B.2 Select a WebLogic Domain Directory



Select the Oracle WebLogic Server directory to which you want to add your applications or services, or both.

Click **Next** to continue.

B.3 Select Domain Source



Select the source from which to create a new Oracle WebLogic Server domain. Select **Generate a domain configured automatically to support the following products** to create your domain to support selected products, and then select the products.

When you select **Oracle Imaging and Process Management**, you should also select **Oracle Universal Content Management - Content Server**.

When you select any Oracle ECM 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 ECM application will also be deselected.

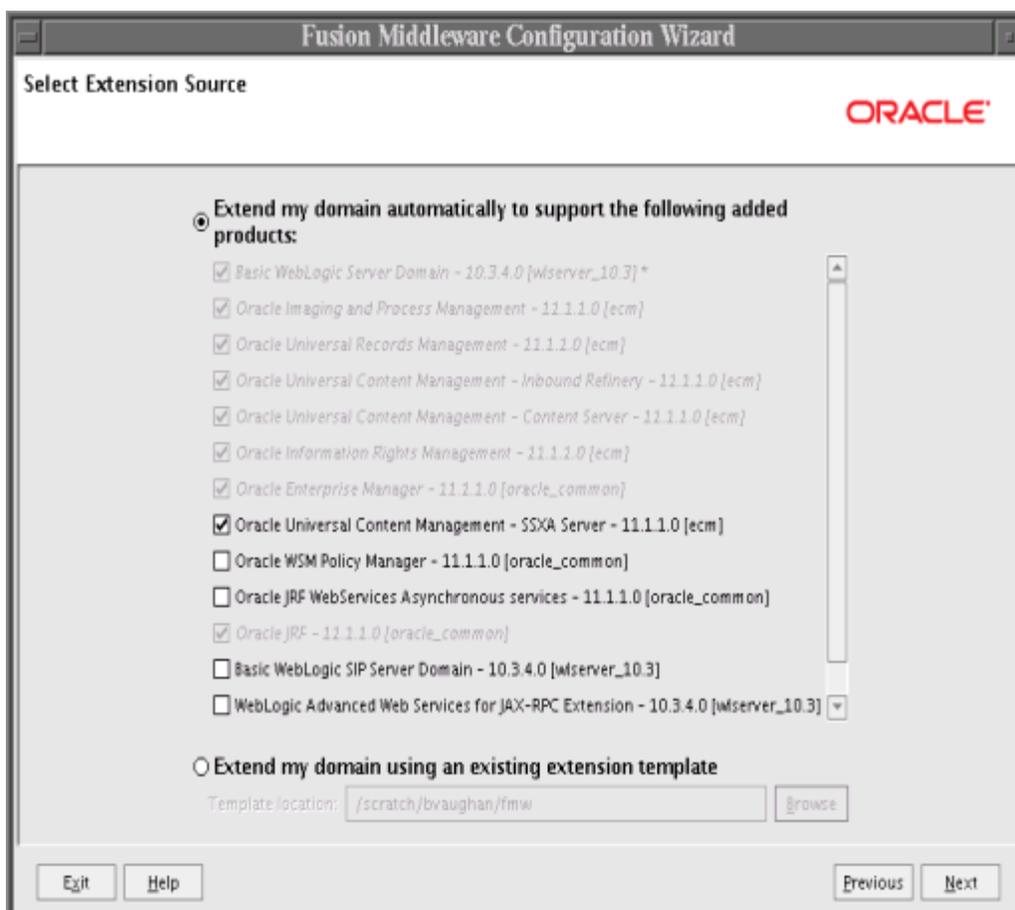
If you want a remote deployment of a Site Studio for External Applications web site, you can select **Oracle Universal Content Management - SSXA Server** to create an Oracle WebLogic Server domain with a Managed Server that has the files required to run the web site.

To create a domain that includes Oracle Web Services Manager (Oracle WSM) Policy Manager, select **Oracle WSM Policy Manager**.

Select **Base this domain on an existing template** to create your domain based on an existing domain template. Click **Browse** to navigate your directories to find an existing template.

Click **Next** to continue.

B.4 Select Extension Source



Select the source from which to extend an existing Oracle WebLogic Server domain. Select **Extend my domain automatically to support the following added products**, and then select the products.

When you select **Oracle Imaging and Process Management**, you should also select **Oracle Universal Content Management - Content Server**, if Oracle UCM is not already configured.

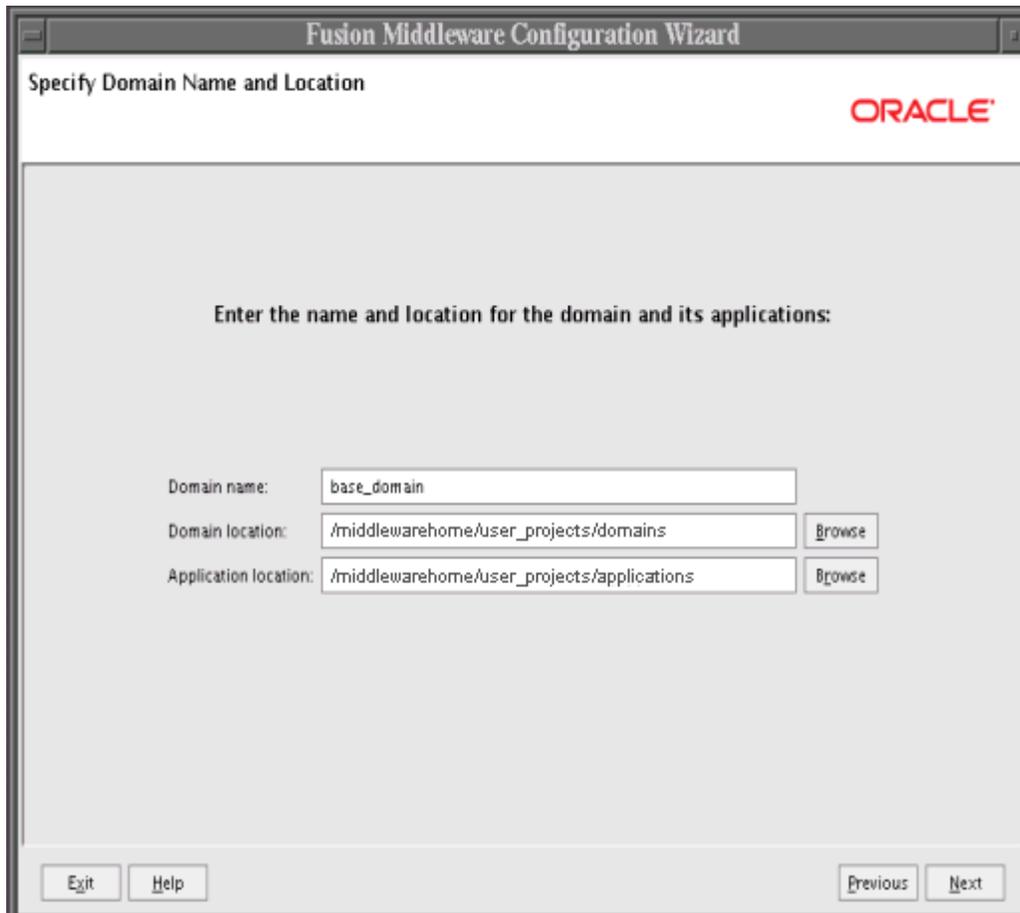
When you select any Oracle ECM application on the Select Extension Source screen, **Oracle Enterprise Manager** and **Oracle JRF** are automatically selected. If you deselect any of these items that are automatically selected, the Oracle ECM application will also be deselected.

If you want a remote deployment for a Site Studio for External Applications web site, you can select **Oracle Universal Content Management - SSXA Server** 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.

B.5 Specify Domain Name and Location

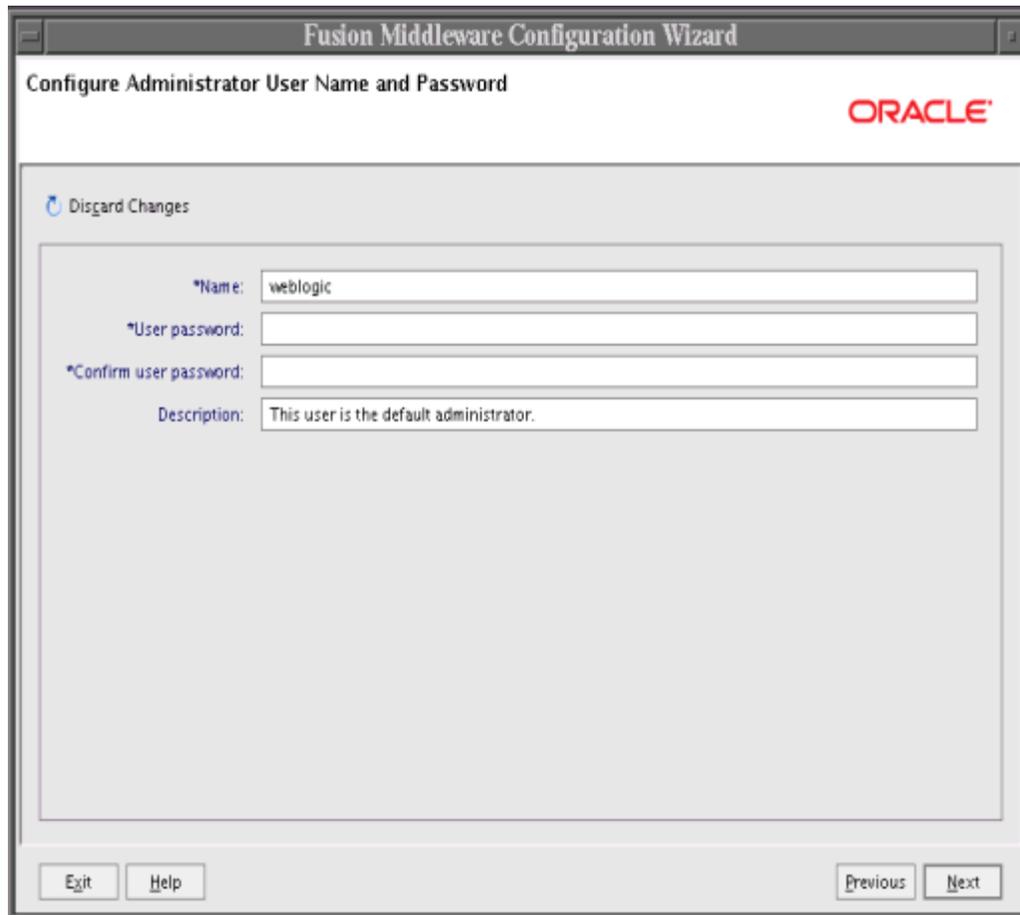


The screenshot shows a window titled "Fusion Middleware Configuration Wizard" with a sub-header "Specify Domain Name and Location" and the Oracle logo. The main area contains the instruction "Enter the name and location for the domain and its applications:". Below this are three input fields: "Domain name:" with the value "base_domain", "Domain location:" with the value "/middlewarehome/user_projects/domains" and a "Browse" button, and "Application location:" with the value "/middlewarehome/user_projects/applications" and a "Browse" button. At the bottom, there are "Exit", "Help", "Previous", and "Next" buttons.

Use the default domain name, domain location, and application location, or specify different ones.

Click **Next** to continue.

B.6 Configure Administrator User Name and Password



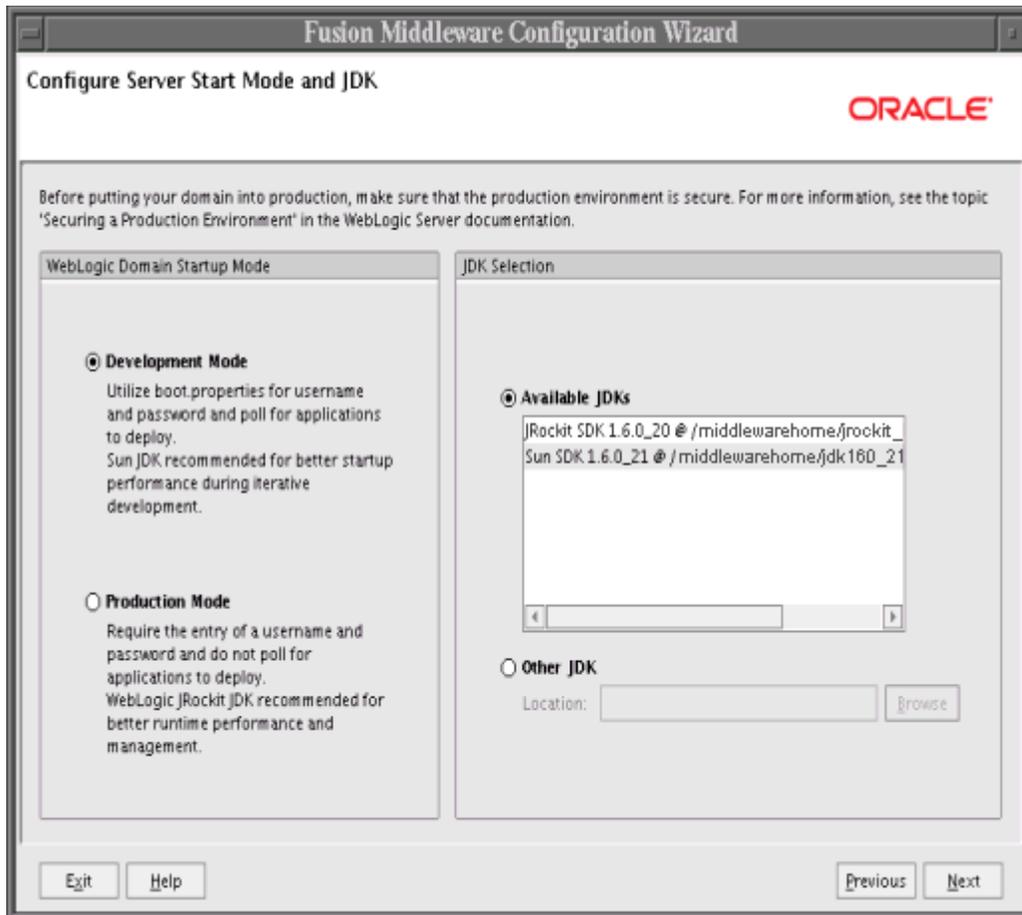
The screenshot shows the 'Configure Administrator User Name and Password' window in the Fusion Middleware Configuration Wizard. The window title is 'Fusion Middleware Configuration Wizard' and the subtitle is 'Configure Administrator User Name and Password'. The Oracle logo is in the top right corner. A 'Discard Changes' button is in the top left. The main area contains four input fields: '*Name:' with the value 'weblogic', '*User password:', '*Confirm user password:', and 'Description:' with the value 'This user is the default administrator.'. At the bottom, there are 'Exit', 'Help', 'Previous', and 'Next' buttons.

Create a user that will be assigned to the Administrator role. This user is the default administrator for starting development mode servers.

- **User name**
Specify the user name.
- **User password**
Specify the password for the user.
- **Confirm user password**
Reenter the user password.
- **Description**
Enter a description for the user. This field is optional.

Click **Next** to continue.

B.7 Configure Server Start Mode and JDK



In the WebLogic Domain Startup Mode section, select one of the following startup modes:

- **Development Mode**

In this mode, `boot.properties` is used for user names and passwords, and polling is used for application deployment. Sun SDK is the default for this mode.

- **Production Mode**

In this mode, user names and passwords are required, and polling is not used for application deployment. JRockit SDK is the default for this mode.

In the JDK Selection section, select a JDK from the list of available JDKs, or select **Other JDK**, and then click **Browse** to find another JDK on your system.

Click **Next** to continue.

B.8 Configure JDBC Component Schema

Note: Change only the input fields below that you wish to modify and values will be applied to all selected rows.

Vendor: DBMS/Service:

Driver: Host Name:

Schema Owner: Port:

Schema Password:

Configure selected component schemas as RAC multi data source schemas in the next panel.

	Component Schema	DBMS/Service	Host Name	Port	Schema Owner	Schema Password
<input type="checkbox"/>	UCM Schema	service_name	dbhost.example.co	1521	DEV_OCS	
<input type="checkbox"/>	IPM Schema	orcl	dbhost.example.co	1521	DEV_IPM	
<input type="checkbox"/>	IRM Schema	orcl	dbhost.example.co	1521	DEV_ORAIRM	
<input type="checkbox"/>	URM Schema	service_name	dbhost.example.co	1521	DEV_URMSERVER	

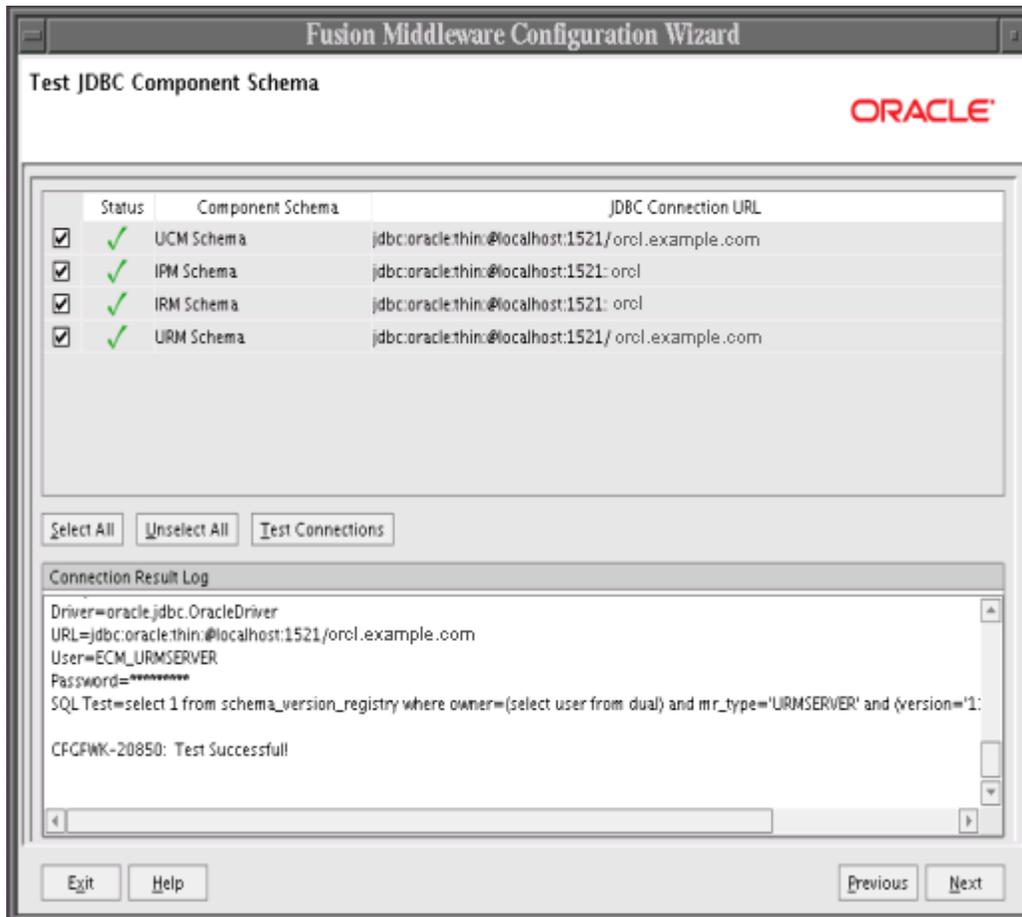
Exit Help Previous Next

Use this screen to edit the configuration information for each JDBC component schema.

A component schema contains a pool of database connections. Your application uses a component schema by looking it up in the JNDI tree, requesting a connection, using the connection, and then returning the connection to the component schema.

Click **Next** to continue.

B.9 Test Component Schema



Use this screen to test JDBC connections to application schemas.

Click **Select All** to select all of the schemas for connection testing, or select one or more individual schemas.

Click **Unselect All** to deselect all of the schemas.

Click **Test Connections** to test the JDBC connections to the selected schema or schemas.

The Connection Result Log section shows the results of connection testing.

Click **Next** to continue.

B.10 Select Optional Configuration



Select any of the server and cluster settings that you want to customize.

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

Click **Next** to continue.

B.11 Configure the Administration Server

The screenshot shows the 'Configure the Administration Server' window in the Fusion Middleware Configuration Wizard. The window title is 'Fusion Middleware Configuration Wizard'. The main title is 'Configure the Administration Server' with the Oracle logo. A 'Disgard Changes' button is at the top left. The configuration fields are: '*Name:' with 'AdminServer', '*Listen address:' with 'All Local Addresses', 'Listen port:' with '7001', 'SSL listen port:' with 'N/A', and 'SSL enabled:' with an unchecked checkbox. At the bottom are 'Exit', 'Help', 'Previous', and 'Next' buttons.

Use this screen to change the default configuration of the Administration Server for an Oracle WebLogic Server domain. Each domain must have one Administration Server, which hosts the Oracle WebLogic Server Administration Console used to perform administration tasks. You can change values in these fields:

- **Name:** The name of the Administration Server
- **Listen Address:** An address on which the Administration Server will listen, selected from the list
- **Listen Port:** The listen port number
- **SSL Listen Port:** The port number for SSL connections, active when **SSL enabled** is selected
- **SSL Enabled:** Enabled if selected and if a port number for SSL connections is provided in the **SSL Listen Port** field

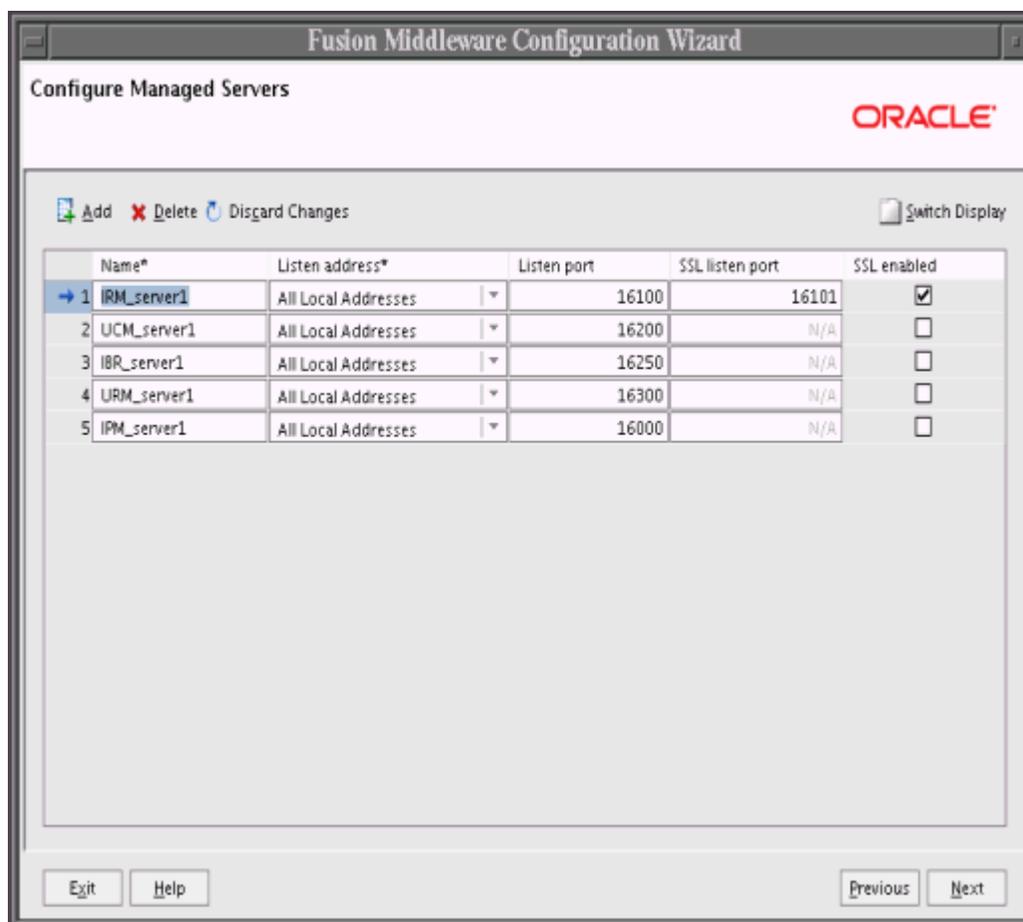
Note: If SSL is enabled, before using Oracle WebLogic Scripting tool (WLST) to connect to the Administration Server, you must append the following parameters to the JVM_ARGS section of the `wlst.sh` file or set them in the `CONFIG_JVM_ARGS` environment variable:

```
-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 ECM Oracle home directory.

Click **Next** to continue.

B.12 Configure Managed Servers



A Managed Server is an instance of Oracle WebLogic Server used to host enterprise applications. A typical production environment has at least one Managed Server.

Use this screen to change the default configuration of Managed Servers. For each Managed Server, you can change values in these columns:

- **Name**
Name of the Managed Server

- **Listen Address**
An address on which the server will listen, selected from the list
- **Listen Port**
Listen port number
- **SSL Listen Port**
Port number for SSL connections, active when **SSL enabled** is selected in the same row
- **SSL Enabled**
Enabled if selected and if a port number for SSL connections is provided in the same row

Click **Next** to continue.

B.13 Configure Clusters



Use this screen to configure Oracle WebLogic Server clusters.

A cluster contains multiple Oracle WebLogic Server instances running simultaneously and working together for scalability and reliability. To clients, a cluster appears as a single Oracle WebLogic Server instance.

Notes:

- To use clusters, you need a license for Oracle WebLogic Server Enterprise Edition.
 - If you configure a cluster, then you must assign a cluster address.
 - If you configure any clusters on the Configure Clusters screen, the Assign Managed Servers to Clusters screen appears next.
-

Click **Next** to continue.

B.14 Assign Servers to Clusters

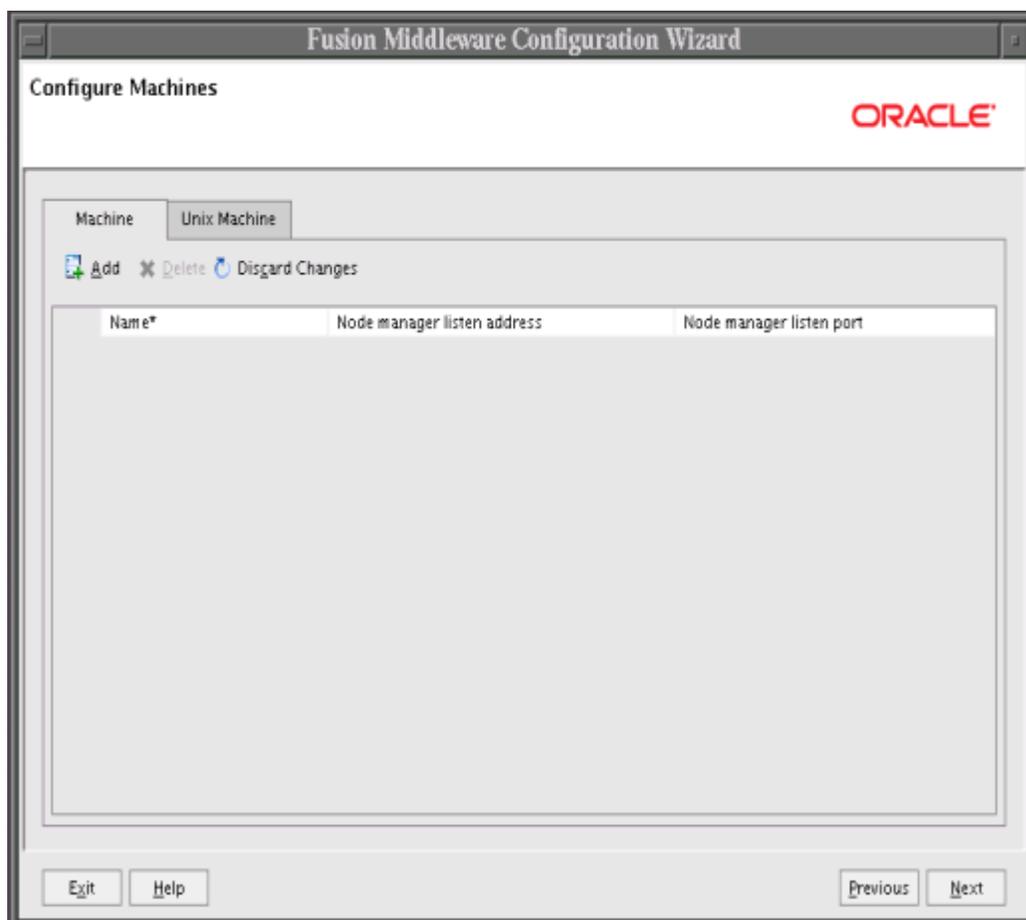
Use this screen to assign Managed Servers to clusters that you added on the Configure Clusters screen.

If you configure a cluster and assign some, but not all, of the Managed Servers in the domain to a cluster, the Create HTTP Proxy Applications screen appears next.

B.15 Create HTTP Proxy Applications

Use this screen to create proxy applications for Managed Servers that you do not assign to a cluster in a domain that includes some clustered Managed Servers.

B.16 Configure Machines

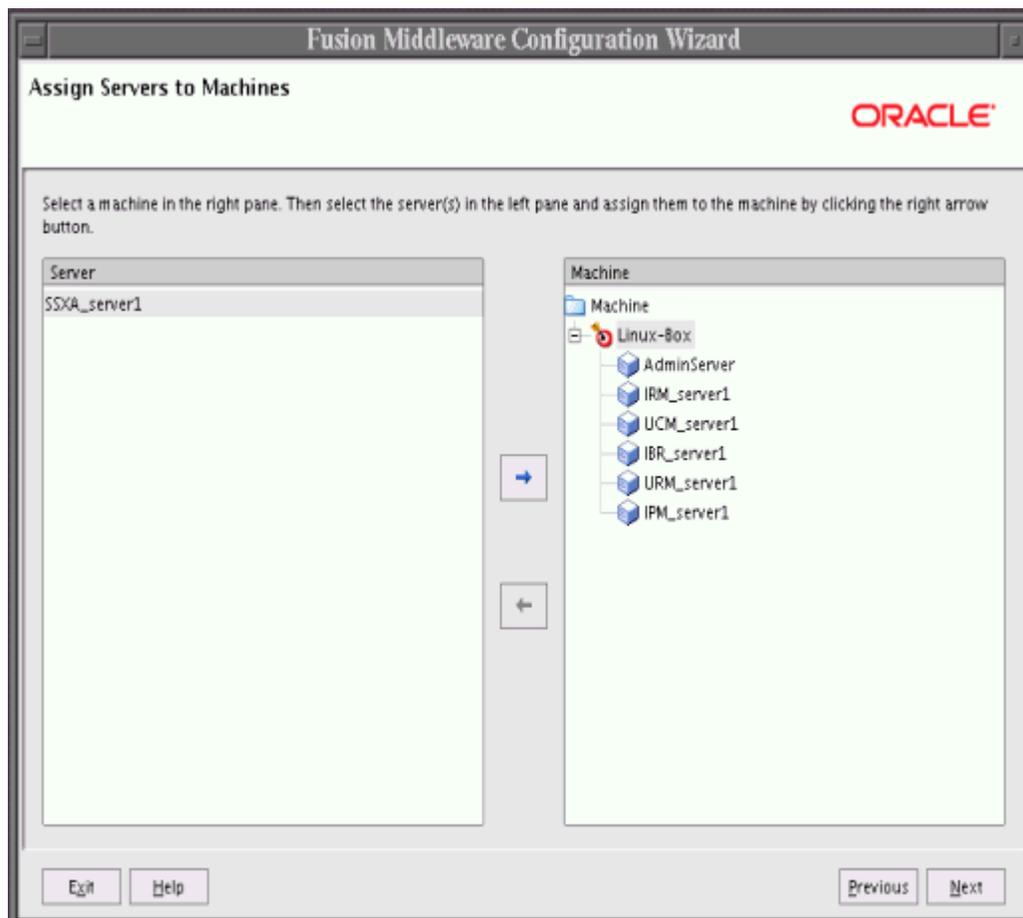


Use this screen to add or delete machines that host Oracle WebLogic Server instances. The Administration Server and Node Manager use the machine configuration on this screen to start remote servers.

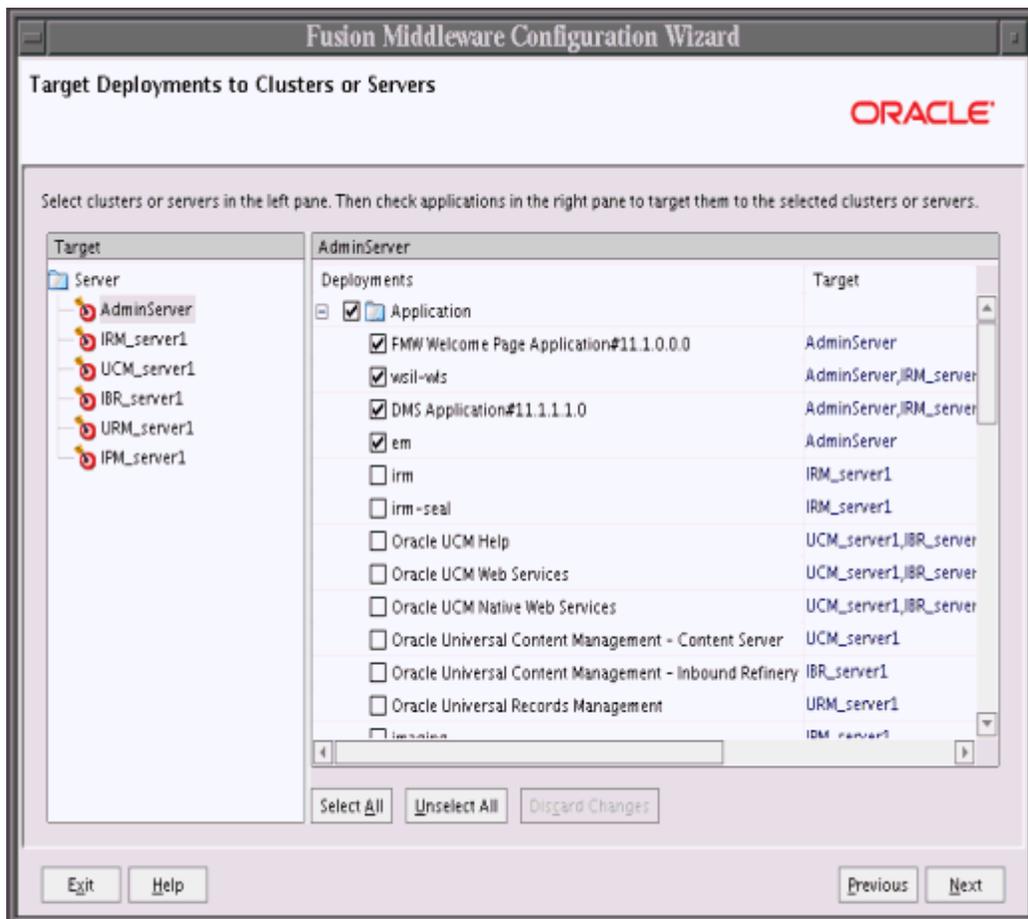
Click **Next** to continue.

B.17 Assign Servers to Machines

Use this screen to assign at least one server to each machine you added on the Configure Machines screen.



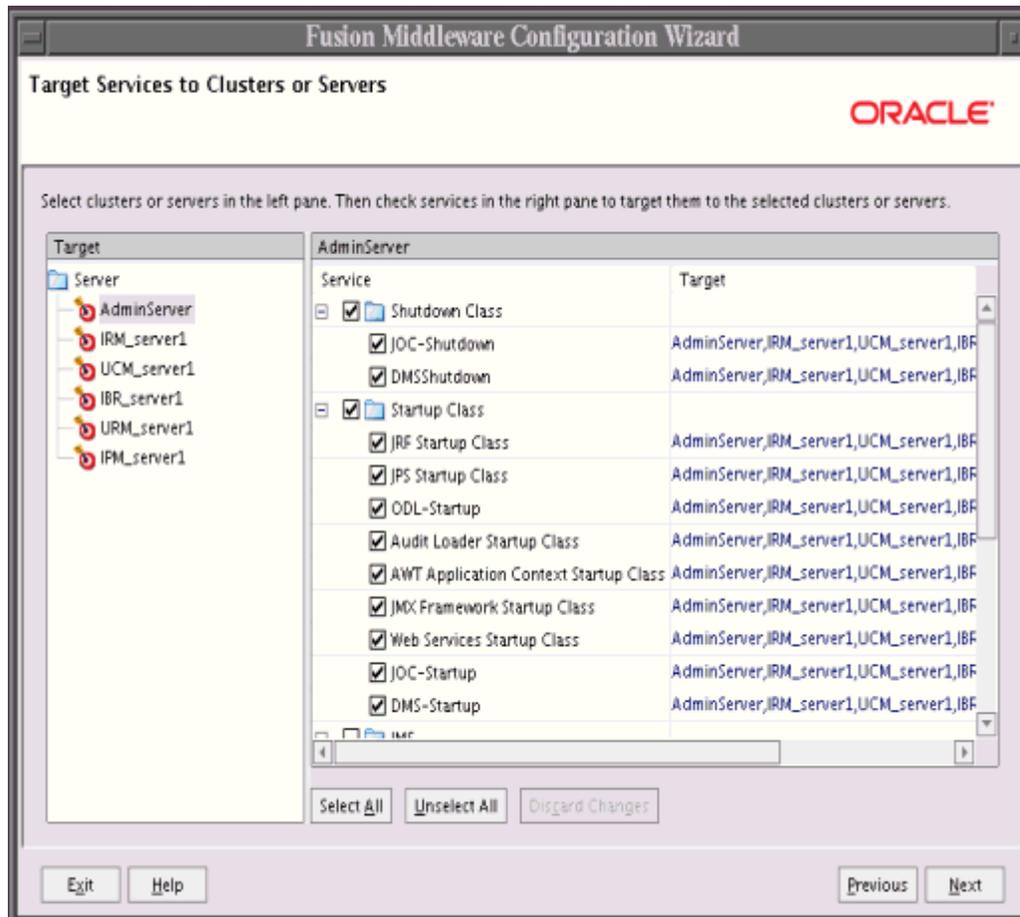
B.18 Target Deployments to Clusters or Servers



Use this screen to target your deployments to Managed Servers or to clusters of Managed Servers. Doing so enables Oracle WebLogic Server to serve the deployments to clients.

Click **Next** to continue.

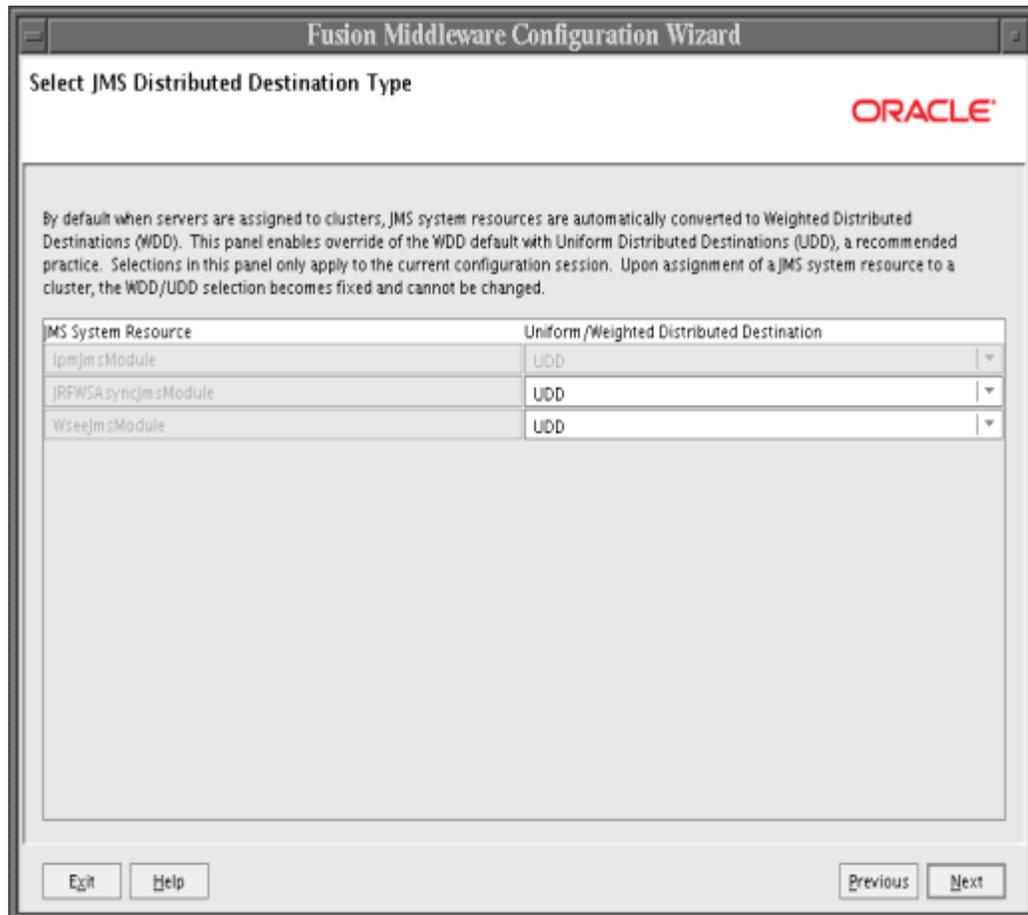
B.19 Target Services to Clusters or Servers



Use this screen to target your services (such as JMS and JDBC) to Managed Servers or to clusters of Managed Servers. Doing so enables your applications to use these services.

Click **Next** to continue.

B.20 Select JMS Distributed Destination Type



Use this screen to select a distributed destination type for JMS.

Click **Next** to continue.

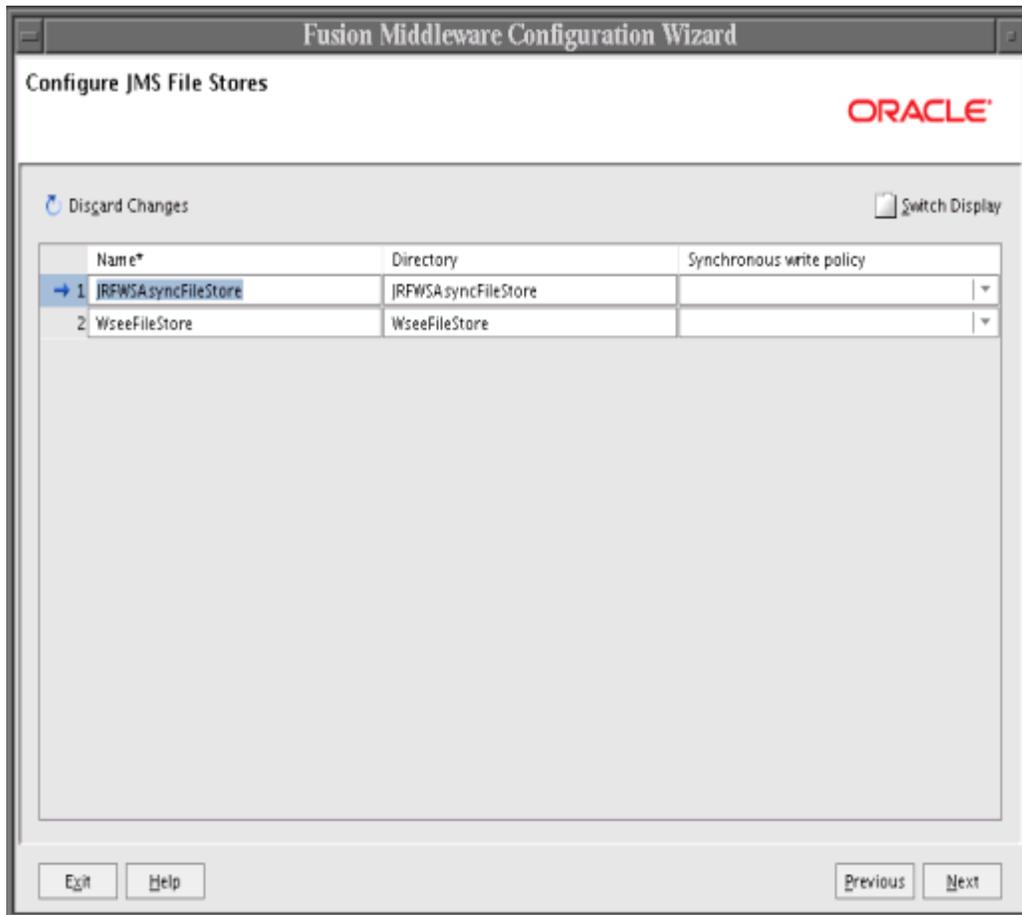
B.21 Configure RDBMS Security Store Database

The screenshot shows the 'Configure RDBMS Security Store Database' window within the 'Fusion Middleware Configuration Wizard'. The window title is 'Fusion Middleware Configuration Wizard' and the subtitle is 'Configure RDBMS Security Store Database'. The Oracle logo is visible in the top right corner. Below the title bar, there are two buttons: 'Discard Changes' (with a refresh icon) and 'Test Connection' (with a test icon). The main instruction reads: 'Create RDBMS tables in data store using scripts in WebLogic Server's server/lib directory.' The form contains several input fields: 'Database Type' (a dropdown menu currently showing 'RDBMS Security Store is Disabled'), 'Driver' (a dropdown menu), 'Class Name' (a text input field), 'DBMS SID' (a text input field), 'User Name' (a text input field), 'DBMS Host' (a text input field), 'User Password' (a text input field), 'DBMS Port' (a text input field), 'Confirm User Password' (a text input field), 'URL' (a text input field), 'Known Properties' (a text input field), and 'Additional Properties' (a text input field with the value 'Optional'). At the bottom of the window, there are four buttons: 'Exit', 'Help', 'Previous', and 'Next'.

Use this screen to make changes to your security store. Make sure that your RDBMS tables are created prior to booting your domain. The scripts used by the DBA are located in the `server/lib` directory under the Oracle WebLogic Server home directory.

Click **Next** to continue.

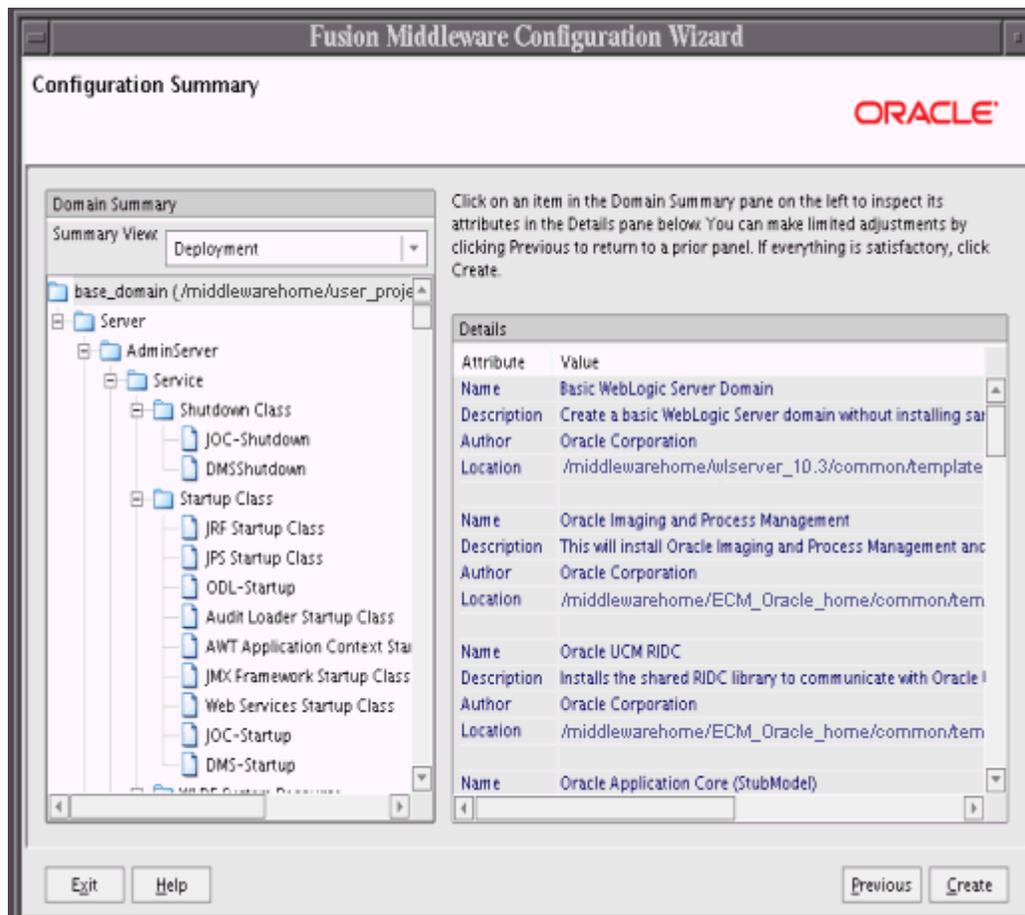
B.22 Configure JMS File Stores



Use this screen to configure JMS file stores for web services.

Click **Next** to continue.

B.23 Configuration Summary

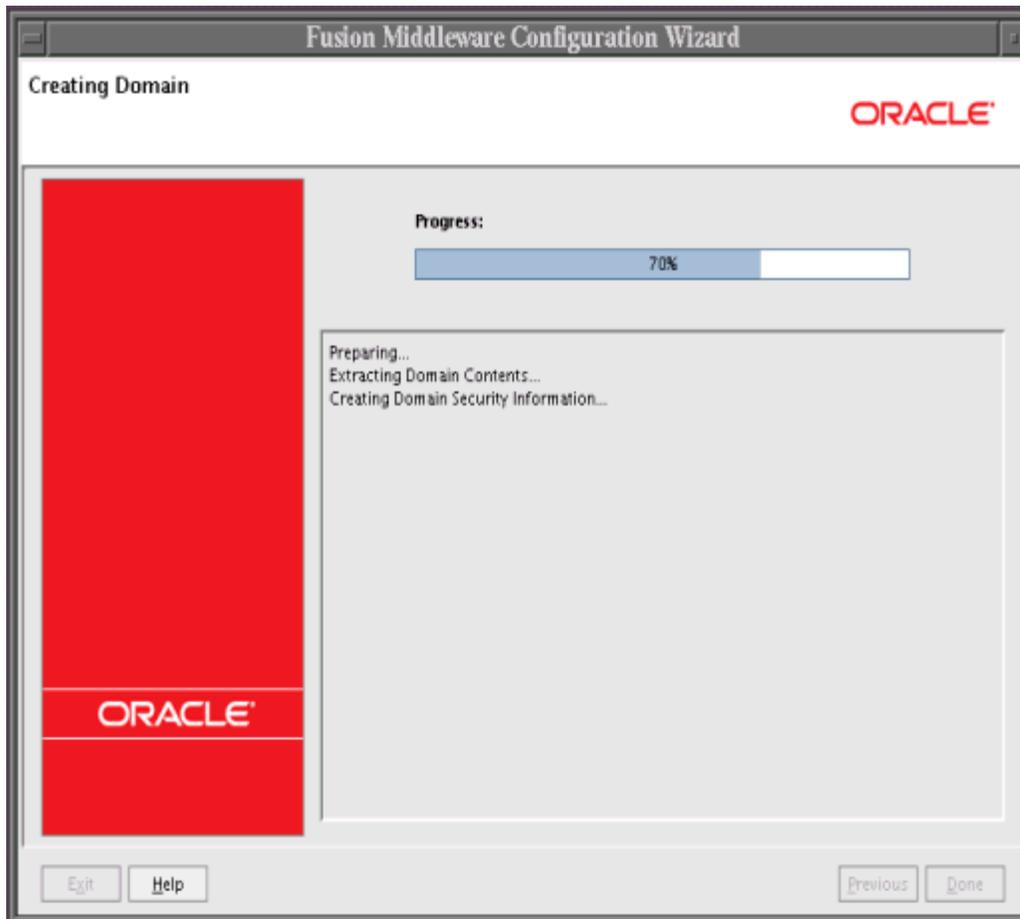


Review the contents of your domain.

Click **Previous** to go back and change something on a preceding screen.

Click **Next** to continue.

B.24 Creating Domain



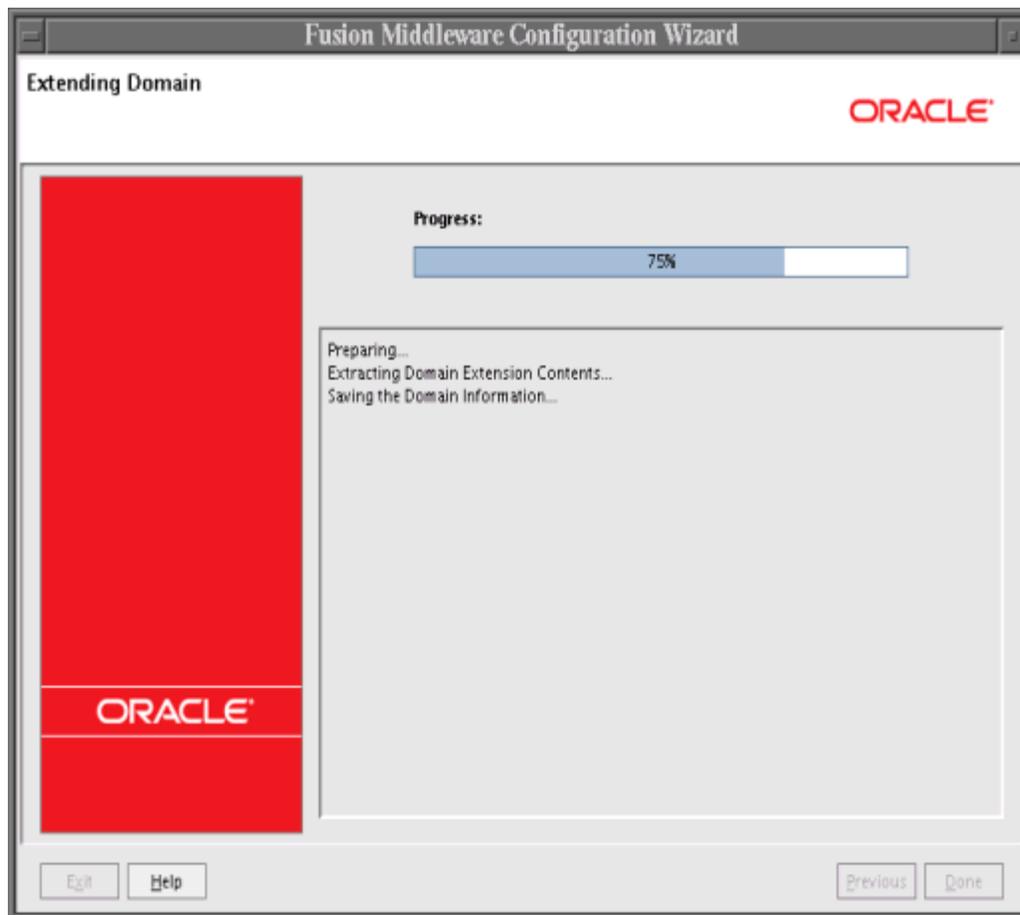
This screen shows the progress of the domain creation.

When the **Progress** bar shows 100%, click **Done** to dismiss the window.

For information about starting the Administration Server and Managed Servers for the domain, see [Section 10.1, "Starting the Administration Server,"](#) and [Section 10.2, "Starting Managed Servers."](#)

On a Windows operating system, you can select **Start Admin Server** on the Creating Domain screen to start the Administration Server for the domain when you click **Done**. This option is not available on a UNIX operating system.

B.25 Extending Domain



This screen shows the progress of the domain extension.

When the **Progress** bar shows 100%, click **Done** to dismiss the window.

For information about starting the Administration Server and Managed Servers for the domain, see [Section 10.1, "Starting the Administration Server,"](#) and [Section 10.2, "Starting Managed Servers."](#)

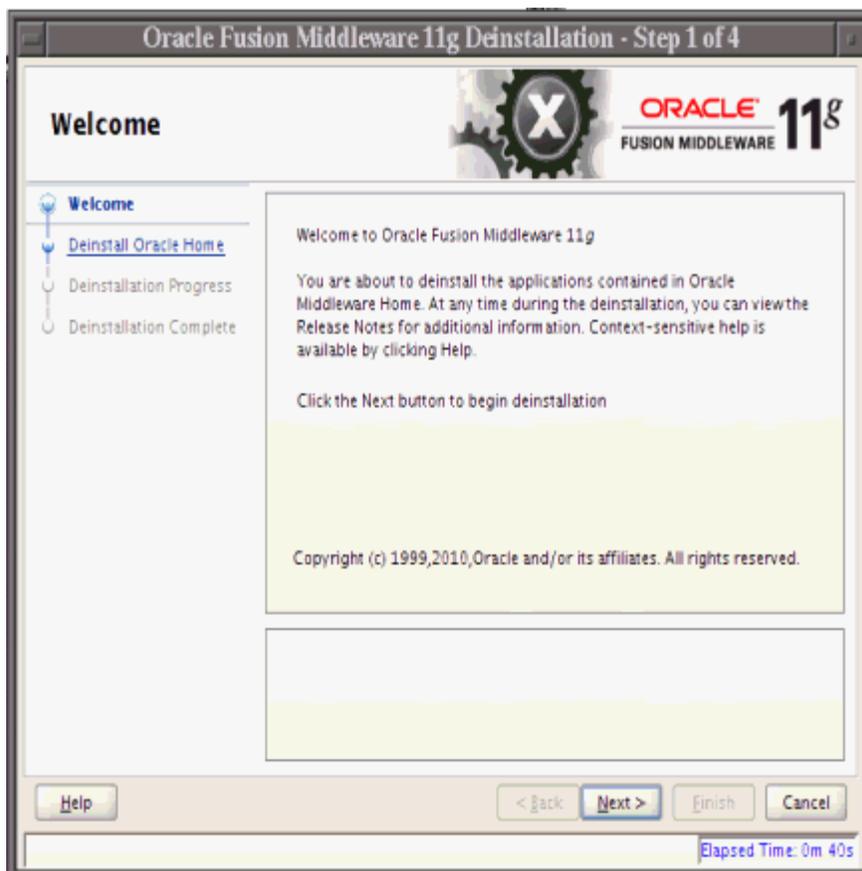
On a Windows operating system, you can select **Start Admin Server** on the Extending Domain screen to start the Administration Server for the domain when you click **Done**. This option is not available on a UNIX operating system.

Deinstallation Screens

This appendix describes screens for deinstalling Oracle Enterprise Content Management Suite:

- [Welcome](#)
- [Deinstall Oracle Home](#)
- [Deinstallation Progress](#)
- [Deinstallation Complete](#)

C.1 Welcome



The Welcome screen is displayed each time you start the deinstaller. Click **Next** to continue.

C.2 Deinstall Oracle Home

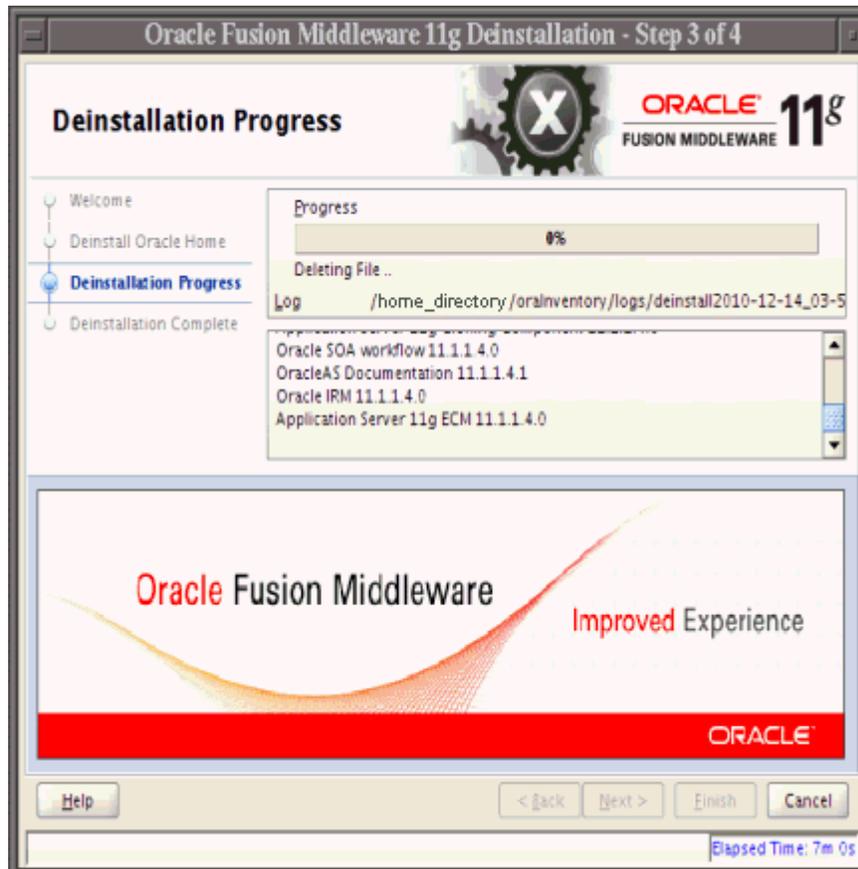


This screen shows the Oracle home directory that is about to be deinstalled. This is the Oracle home directory from which the deinstaller was started.

Note: Before you choose to remove this Oracle home, make sure that it is not in use by an existing domain.

Verify that this is the correct directory, then click **Deinstall** to continue.

C.3 Deinstallation Progress



This screen shows you the progress of the deinstallation.

If you want to quit before the deinstallation is completed, click **Cancel**.

C.4 Deinstallation Complete



This screen summarizes the deinstallation that was just completed.

Click **Finish** to dismiss the screen.

Troubleshooting

This appendix provides troubleshooting information, in these topics:

- [General Troubleshooting Tips](#)
- [Suite Installation and Configuration Troubleshooting](#)
- [Oracle Inbound Refinery Problems](#)
- [Additional Help](#)

D.1 General Troubleshooting Tips

If you encounter an error during installation:

- Read the *Oracle Fusion Middleware Release Notes for Microsoft Windows (32-Bit)* for the latest updates. The release notes are available with the platform-specific documentation. The most current version of the release notes is available from the Oracle Documentation page on Oracle Technology Network at <http://www.oracle.com/technology/documentation>
- Verify that your system meets the requirements specified in [Section 3.1.1, "Meeting System Requirements"](#).
- If you are installing a middle tier, check that the OracleAS Infrastructure with which you want to associate the middle tier is running during installation.
- If you entered incorrect information on one of the installation screens, return to that screen by clicking **Back** until you see the screen.
- If an error occurred while the installer is copying or linking files:
 1. Note the error and review the installation log files.
 2. Remove the failed installation by following the steps in [Chapter 11, "Deinstalling Oracle Enterprise Content Management Suite."](#)
 3. Correct the issue that caused the error.
 4. Restart the installation.

D.2 Suite Installation and Configuration Troubleshooting

This section contains solutions to common problems that you might encounter while installing and configuring Oracle Enterprise Content Management Suite.

If you are having problems with full-text search, Oracle IBR conversions, Dynamic Converter, Desktop Integration Suite, 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 4.7.3, "Downloading Visual C++ Libraries for a Windows Operating System."](#)

D.2.1 Oracle Fusion Middleware Installation and Configuration Log Files

The Oracle Fusion Middleware 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/installActionstimestamp.log`
 - `oraInventory_location/logs/oraInstalltimestamp.err`
 - `oraInventory_location/logs/oraInstalltimestamp.out`
 - `ORACLE_HOME/install/make.log`
- On a Windows operating system, the installer writes the following log files:
 - `inventory_location\logs\installActionstimestamp.log`
 - `inventory_location\logs\oraInstalltimestamp.err`
 - `inventory_location\logs\oraInstalltimestamp.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.

D.2.2 Oracle IRM Key Store Configuration Issues

If the Oracle Information Rights Management (Oracle IRM) 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
```

D.2.3 Oracle I/PM Errors During Attempt to Connect to Oracle UCM 11g

When you attempt to connect Oracle I/PM to an Oracle UCM 11g repository, Oracle I/PM returns errors in these cases:

- If Oracle UCM is installed in a domain that is later extended with Oracle I/PM and you have not restarted the Oracle I/PM Managed Server.
- If the Oracle UCM and Oracle I/PM 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 7.1.1.1, "Configuring Oracle Content Server 11g to Work with Oracle I/PM."](#)

D.3 Oracle Inbound Refinery Problems

If you are having problems with Oracle IBR 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 4.7.3, "Downloading Visual C++ Libraries for a Windows Operating System."](#)

This section provides troubleshooting information for the following Oracle IBR setup and run issues:

- [Oracle IBR Will Not Run As an Application or Service](#)
- [Oracle IBR Runs As an Application But Not As a Service](#)
- [Oracle IBR Service Keeps Stopping](#)
- [Cannot Log In to Refinery After Installation](#)
- [Files Intermittently Stuck in GenWWW Status](#)
- [Oracle IBR Service Will Not Convert Documents](#)

D.3.1 Oracle IBR Will Not Run As an Application or Service

Oracle IBR will not run as either an application or a service. If you try to run Oracle IBR 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 Oracle IBR machine. Sun Java must be installed on both the Oracle Content Server machine and the Oracle IBR machine.	<ul style="list-style-type: none"> Reinstall Oracle IBR to reinstall the Sun JVM. Copy the Sun Java files from the Oracle Content Server machine to the Oracle IBR machine. Open the <code>intradoc.cfg</code> file located in the <code>refinery_install_dir\bin</code> directory and make sure the <code>JAVA_EXE</code> 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 Oracle IBR machine. Open the <code>intradoc.cfg</code> file located in the <code>refinery_install_dir\bin</code> directory and make sure the <code>JAVA_EXE</code> path is correct.

D.3.2 Oracle IBR Runs As an Application But Not As a Service

Oracle IBR 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 Oracle IBR service has not been given the right to log on as a service.	Make sure user linked to the Oracle IBR service is valid and has the right to log on as a service.
There is a problem with the Oracle IBR service.	<ul style="list-style-type: none"> Reboot the Oracle IBR machine. Try running Oracle IBR as an application, then retry running it as a service. Sometimes running Oracle IBR as an application once will clear up problems with the service. Delete and re-add the service in Oracle IBR

D.3.3 Oracle IBR Service Keeps Stopping

The Oracle IBR 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 <code>intradoc.cfg</code> file for the refinery.	Change the Java options settings in the <code>intradoc.cfg</code> file for the Oracle IBR 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 Oracle IBR 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 Oracle IBR service.

D.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 Oracle Content Server, but the InboundRefinerySupport component has not been installed and enabled on Oracle Content Server.	Install and enable the InboundRefinerySupport component on Oracle Content Server. For more information, see Section 6.2.3.2, "Enabling Components for Oracle IBR on Oracle Content Server."

D.3.5 Files Intermittently Stuck in GenWWW Status

When Oracle UCM 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
<p>The problem is directly related to known file locking and deleting issues on a Windows Server 2003 system and typically occurs when Oracle 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 Oracle IBR on the Windows Server 2003 system and Oracle IBR resides on a separate physical machine from Oracle Content Server.</p> <p>For more information about these Windows Server 2003 issues, see knowledge base articles 885451 and 811492 on the Microsoft Support web site at</p> <p>http://support.microsoft.com http://support.microsoft.com</p>	<p>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.</p> <ol style="list-style-type: none"> 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 <i>opportunistic locking</i> 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. <p>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</p> <p>http://support.microsoft.com</p>

D.3.6 Oracle IBR Service Will Not Convert Documents

You are running Oracle IBR as a service, but it will not convert any documents, and the following error message is displayed in the Oracle IBR log:

```
Unable to convert, native application reported: 'Permission denied'
```

This error will usually occur when Samba is used with Oracle Content Server on a UNIX operating system or with Oracle IBR on a Windows operating system.

Possible Causes	Solutions
<p>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 Oracle IBR service.</p>	<p>Change the DCOM permissions for the user running the Oracle IBR service. For details, see the following procedure for changing DCOM permissions.</p>

To change DCOM permissions:

1. Launch `dcemocnfg.exe` to check user permissions for the user running the Oracle IBR service.
2. On the **Default Security** tab, make sure the domain user is added to **Connect, Access, Launch, and Configuration**.
3. Restart the Oracle IBR service.

D.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 *OracleMetaLink*) web site at <http://support.oracle.com>

If you do not find a solution for your problem, open a service request.

Index

A

accessibility software, Java Access Bridge, A-1, B-1
adding users, Oracle Internet Directory, 4-35
Administration Server, starting, 10-1
administrator user, 7-5
Administrators group, 7-5
AES algorithm, 8-3
allowing IMPORT definitions in Oracle I/PM, 7-9
applications
 Oracle Enterprise Content Management Suite, 1-1
 Oracle Imaging and Process Management, 1-1
 Oracle Inbound Refinery, 1-1
 Oracle Information Rights Management, 1-2
 Oracle Universal Content Management, 1-1
 Oracle Universal Records Management, 1-2
Assign Servers to Clusters screen, B-15
Assign Servers to Machines screen, B-17
AXF. *See* Oracle Application Extension Framework

C

certification, 3-1
chmod command, symbolic link to, 3-8
client configuration, server certificate, 4-26
clusters
 configuration screens, 4-40
 configuring, 4-40
 Managed Servers, 4-39
Configuration
 Desktop Integration Suite, client workstation, 5-17
 Oracle Content Server, 5-3
 Oracle URM, 9-1
configuration
 clusters, 4-40
 desktop authentication, 4-37
 Desktop Integration Suite on client workstation, 9-7
 external database provider for standalone applications, 5-10
 Java Object Cache for AXF in distributed Oracle I/PM servers, 7-11
 JDBC Driver for standalone applications, 5-10
 key store for Oracle IRM, 8-2
 log, D-2

 machines, 4-40
Managed Servers
 clusters, 4-39, 4-40
 creating Oracle WebLogic Server domain, 4-3
 extending Oracle WebLogic Server domain, 4-10
 machines, 4-40
Microsoft SQL Server with Oracle UCM, 5-7
Oracle Access Manager, 4-37
Oracle Access Manager 11g for Oracle IRM Managed Server, 8-8
Oracle Application Extension Framework, 5-19, 7-11
Oracle Content Server
 Content Server Configuration page, 5-4
 Desktop Integration Suite, 5-16
 Oracle Text Search, 5-8
 Site Studio, 5-12
 with Oracle I/PM, 7-3
Oracle Distributed Document Capture, 5-20
Oracle Document Capture, 5-20
Oracle Enterprise Content Management Suite, 4-1
Oracle Imaging and Process Management
 allowing IMPORT definitions, 7-9
 overview, 7-1
Oracle Inbound Refinery
 document conversion, 6-5
 overview, 6-1, 6-2
 postinstallation, 6-2
Oracle Information Rights Management
 overview, 8-1
 single sign-on, 8-8
Oracle Text Search, configuring for Oracle Content Server, 5-8
Oracle UCM repository, 7-3
Oracle Universal Content Management, 5-1
Oracle URM Adapter for Oracle UCM, 5-17
preparing for, 4-1
screens, B-1
single sign-on for Oracle IRM Managed Server, 8-8
Site Studio on Oracle Content Server, 5-12
troubleshooting, D-2
verifying, 10-1
Windows Native Authentication, 4-39
zone fields, 5-14

- Configuration Summary screen, B-23
- Configure Administrator User Name and Password screen, B-7
- Configure Clusters screen, B-14
- Configure JDBC Component Schema screen, B-9
- Configure JMS File Stores screen, B-22
- Configure Machines screen, B-16
- Configure Managed Servers screen, B-13
- Configure RDBMS Security Store Database screen, B-21
- Configure Server Start Mode and JDK screen, B-8
- Configure the Administration Server screen, B-12
- configuring 10g server to work with Oracle I/PM, 7-3
- connections
 - Oracle I/PM to Oracle UCM repository, 7-7
 - Oracle I/PM to workflow server, 7-10
- Content Server Configuration page, 5-4
- Content Server. *See* Oracle Content Server
- conversion components, enabling on Oracle IBR, 6-5
- conversion jobs, Oracle IBR, setting up, 6-6
- Create HTTP Proxy Applications screen, B-15
- createCentralInventory.sh script, 3-9
- Creating Domain screen, B-24
- Creating Domain screen (extending domain), B-25
- creating Oracle WebLogic Server domain, 4-3, 4-4
- creating schemas, 2-1, 2-2
- credential store, configuring for Oracle IRM, 8-7
- cryptographic algorithm for key store
 - AES, 8-3
 - choosing, 8-3
 - RSA, 8-3

D

- data sources
 - IBM DB2, 9-7
 - Microsoft SQL Server, 5-7
- database
 - creating schemas, 1-8, 2-1, 2-2
 - IBM DB2, 1-4
 - installation module, 1-8
 - Microsoft SQL Server
 - configuration with Oracle UCM, 5-7
 - creating schemas in, 1-4
 - Oracle Database, 1-4, 1-8
 - Repository Creation Utility
 - compatibility, 1-8
 - prerequisites, 2-1
 - schemas, 1-8, 2-1
 - supported, 1-8
- database root CA certificate, 5-12
- default ports for Managed Servers, 4-9
- default project document information, 5-14
- Deinstall Oracle Home screen, C-3
- Deinstallation Complete screen, C-5
- deinstallation procedure, 11-4
- Deinstallation Progress screen, C-4
- deinstallation screens, C-1

- deinstalling Oracle Enterprise Content Management Suite
 - overview, 11-1
 - procedure, 11-3
 - tasks, 11-1
- desktop authentication, configuring, 4-37
- Desktop Integration Suite
 - configuration, client workstation, 5-17, 9-7
 - installation, client workstation, 5-17, 9-7
 - Oracle Content Server configuration, 5-16
- DHCP host
 - configuring, 3-5
 - UNIX operating system, 3-5
 - Windows operating system, 3-5
- directory structure, 1-9
- disabling web layout for Oracle I/PM, 7-7
- distributed Oracle I/PM servers, configuring Java Object Cache for AXF, 7-11
- document conversion, configuring on Oracle IBR, 6-5
- domain structure, Oracle WebLogic Server, 1-9
- domains
 - creating, 4-3
 - extending, 4-10, 4-11, 4-15
- downloads, Oracle ECM software, 1-2
- dropping schemas, 11-3
- DynamicSections property
 - connection pool configuration, 9-7
 - setting in IBM DB2 and Oracle URM, 9-7

E

- ECM. *See* Oracle Enterprise Content Management Suite
- email address, system administrator, 5-6
- Enabled Features page, 9-1
- enabling JSP groups on Oracle Content Server, 5-15
- enabling JSP support on Oracle Content Server, 5-15
- enabling Site Studio on Oracle Content Server, 5-12, 5-13
- environment variables
 - library paths, UNIX platforms, 4-22
 - Outside In Technology, 4-19
- errors, Oracle I/PM connection to Oracle UCM 11g, D-3
- extending an existing domain, 4-10, 4-11, 4-15
- external database provider, configuration for standalone applications, 5-10
- external LDAP authentication provider, 4-27

F

- file formats, selecting for Oracle IBR conversion, 6-8
- file store provider
 - configuring for Oracle Content Server, 7-6
 - configuring for Oracle I/PM, 7-6
- fonts
 - installing, UNIX operating system, 4-18, 4-19
 - National Language Support, UNIX operating system, 4-36

full-text features, configuring in Oracle UCM, 7-10
full-text indexing
 in metadata fields, 5-14
 zone fields, 5-14

G

GDFontPath MBean, configuring for Oracle
I/PM, 7-8

H

heap size, increasing, 4-16
HelloBpel Solution, 7-13
HelloWorld Solution, 7-12
HttpServerAddress, 5-5, 6-4

I

IBM DB2, 1-4
 database searches, 5-7
 DynamicsSections property, setting for Oracle
 URM, 9-7
IBR. *See* Oracle Inbound Refinery
identity store
 configuring for Oracle IRM, 8-8
 reassociating with external LDAP, 4-27
 reassociating with Oracle Internet Directory, 4-27
IMPORT definitions, allowing in Oracle I/PM, 7-9
importing into key store, 5-12
Inbound Refinery Configuration page, 6-3
Inbound Refinery. *See* Oracle Inbound Refinery
Incoming Socket Connection Address Security
 Filter, 4-41
increasing Java heap size for Managed Servers, 4-16,
 10-6
Install Software Updates screen, A-3
installation
 default project document information, 5-14
 Desktop Integration Suite, client
 workstation, 5-17, 9-7
 enabling JSP groups on Oracle Content
 Server, 5-15
 enabling JSP support on Oracle Content
 Server, 5-15
 enabling Site Studio on Oracle Content
 Server, 5-12, 5-13
 log, D-2
 modules
 database, 1-8
 Oracle Enterprise Content Management
 Suite, 1-8
 Oracle WebLogic Server, 1-7
 overview, 1-7
 Repository Creation Utility, 1-8
 multihomed computer, 3-7
 non-networked computer, 3-7
 Oracle Access Manager 11g, 8-8
 Oracle Application Extension Framework, 7-11
 Oracle Application Extension Framework, with
 Oracle I/PM, 5-19

Oracle Distributed Document Capture, 5-20
Oracle Document Capture, 5-20
Oracle Enterprise Content Management
 Suite, 3-1, 3-7, 3-9, 3-10, 4-41
Oracle Imaging and Process Management, 3-7
Oracle Inbound Refinery, overview, 6-2
Oracle Information Rights Management, 3-7
Oracle URM Adapter for Oracle UCM, 5-17
Oracle WebLogic Server, 3-2, 4-41
 overview, 1-1
 preparing for, 3-1
 procedure, 1-4
 roadmap, 1-3
 screens, A-1
 troubleshooting, D-2
 verifying, 7-11, 10-1, 10-6
 zone fields, 5-14

Installation Completed screen, A-8
installation log files, 3-8
Installation Progress screen, A-7
Installation Summary screen, A-6
installer, starting, 3-8
installing fonts
 National Language Support, 4-19
 UNIX operating system, 4-18
InstanceDescription property, 5-6
InstanceMenuLabel property, 5-6
interface
 Enabled Features Page, 9-1
 Oracle URM Setup Checklist, 9-4
inventory directory location, 3-9
IPM. *See* Oracle Imaging and Process Management
IRM. *See* Oracle Information Rights Management

J

Java Access Bridge (Windows operating system), 3-4
Java heap size, increasing for Managed Server, 10-6
Java Object Cache for AXF, configuring for
 distributed Oracle I/PM servers, 7-11
Java VM memory parameters, 4-17
JavaServer Pages
 enabling on Oracle Content Server, 5-15
 JSP groups, 5-15
JDBC driver configuration for standalone
 applications, 5-10
JDK version, upgrading in Oracle Content Server
 10g, 7-3
JRE locations, 3-9

K

key size, 8-3
key store, 4-42
 adding passwords to the credential store, 8-6
 configuration issues, D-2
 configuring for Oracle IRM, 8-2
 creating for Oracle IRM, 8-3
 cryptographic algorithm, 8-3

- importing database root CA certificate, standalone applications, 5-12
- key size, 8-3
- setting location, 8-4
- setting up, 4-42
- target platform, 8-3

L

- LDAP authenticator types, 4-28
- libraries for Outside In Technology
 - installing, 4-19
 - UNIX platform
 - environment variables, 4-22
 - installing, 4-19
 - Windows operating system, downloading Visual C++, 4-22
- log files, installation, 3-8
- loopback adapter (Windows operating system)
 - installing, 3-5
 - removing, 3-6

M

- machines, configuring, 4-40
- Managed Servers
 - cluster configuration, 4-39
 - configuration
 - clusters, 4-40
 - Java heap size, 10-6
 - default ports, 4-9
 - increasing Java heap size, 10-6
 - Oracle Inbound Refinery, 6-2
 - document conversion configuration, 6-5
 - installation, 6-2
 - Oracle I/PM
 - configuring Oracle UCM repository, 7-2
 - Java Object Cache for AXF, 7-11
 - restarting, 10-4
 - starting, 7-5, 7-7, 10-2
- MBeans, configuring for Oracle I/PM, 7-8
- memory parameters, Java VM, 4-17
- metadata fields for Site Studio, 5-14
- metadata for project files, 5-14
- Microsoft SQL Server
 - configuration with Oracle UCM, 5-7
 - creating schemas in, 1-4
- Middleware home, 1-7, 3-2
- multihomed computer, installation on, 3-7

N

- National Language Support, fonts, UNIX operating system, 4-36
- Node Manager, starting, 10-5
- non-networked computer, installation on, 3-7

O

- Oracle Access Manager
 - configuring, 4-37, 8-8
 - installing for Oracle IRM, 8-9
- Oracle Access Manager 11g
 - installing, 8-8
 - single sign-on, 8-8
- Oracle Application Extension Framework
 - configuration, 5-19, 7-11
 - installation, 7-11
 - installation with Oracle I/PM, 5-19
 - verifying installation, 7-11
- Oracle AXF. *See* Oracle Application Extension Framework
- Oracle Common home, 1-7
- Oracle Content Server, 7-3
 - configuration, 5-3, 7-3
 - Desktop Integration Suite, 5-16
 - file store provider, 7-6
 - Oracle Text Search, 5-8
 - configuration page, 5-4
 - configuring to work with Oracle I/PM, 7-2
 - enabling Oracle Inbound Refinery components, 6-7
 - file store provider configuration, 7-6
 - initial configuration, 5-3
 - JavaServer Pages, 5-15
 - JSP groups, 5-15
 - repository for Oracle I/PM, 7-3
 - search index, 5-16
 - Site Studio, 5-12, 5-13
 - SiteStudioExternalApplications component, 5-12, 5-13
 - starting, 5-3
 - upgrading JDK version for 10g server, 7-3
- Oracle Database, 1-8
 - creating schemas in, 1-4
 - patch for 11.1.0.7.0 with Oracle Text 11g, 5-9
- Oracle Distributed Document Capture
 - configuration, 5-20
 - installation, 5-20
- Oracle Document Capture, 7-15
 - configuration, 5-20
 - installation, 5-20
- Oracle ECM. *See* Oracle Enterprise Content Management Suite
- Oracle E-Delivery software downloads, 1-2
- Oracle Enterprise Content Management Suite
 - applications, 1-1
 - configuration screens, B-1
 - configuring, 4-1
 - deinstallation procedure, 11-4
 - deinstalling, 11-1, 11-3
 - directory structure, 1-9
 - installation, 3-7, 3-9, 4-41
 - in Oracle Fusion Middleware, 3-1
 - module, 1-8
 - procedure, 3-10
 - screens, A-1

- preparing for configuration, 4-1
- schemas, 1-4, 2-2
- starting Managed Servers, 10-2
- verifying installation and configuration, 10-1, 10-6
- Oracle Fusion Middleware
 - Middleware home, 1-7
 - Oracle WebLogic Server installation, 1-7
 - stopping, 11-1
- Oracle homes
 - in Middleware home, 1-7
 - removing directories, 11-4
- Oracle IBR. *See* Oracle Inbound Refinery
- Oracle Imaging and Process Management, 1-1, 7-7
 - configuration
 - after first login, 7-1
 - allowing IMPORT definitions, 7-9
 - application, 7-1
 - Java Object Cache for AXF in distributed servers, 7-11
 - Oracle Access Manager 11g, 8-8
 - Oracle UCM repository, 7-2
 - repository, 7-3
 - single sign-on, 8-8
 - configuring Oracle Content Server, 7-2
 - connecting to workflow server, 7-10
 - disabling web layout for Oracle I/PM, 7-7
 - errors, connection to Oracle UCM, D-3
 - installing, 3-7
 - Oracle Application Extension Framework, 5-19
 - Oracle Content Server 10g configuration, 7-3
 - Oracle UCM repository, 7-2
 - postinstallation configuration, 7-1
 - repository connection, 7-7
 - resetting system security, 7-10
 - starting Managed Server, 7-5, 7-7
 - Visual C++ package for Windows operating system, 4-22
 - web client, 7-5, 7-7
- Oracle Inbound Refinery, 1-1
 - configuration
 - document conversion, 6-5
 - overview, 6-1, 6-2
 - conversion jobs
 - from Oracle Content Server, 6-6
 - setting up, 6-6
 - enabling components on Oracle Content Server, 6-7
 - enabling conversion components, 6-5
 - enabling PDFExportConverter, 6-5
 - Oracle Content Server, setting up jobs for conversion, 6-6
 - outgoing provider from Oracle Content Server, 6-6
 - postinstallation configuration, 6-1, 6-2
 - selecting file formats for conversion, 6-8
 - setup and run issues, D-3
 - troubleshooting
 - conversion errors, D-6
 - login errors, D-5
 - problems, D-3
 - runtime errors, D-3, D-4, D-5
- Oracle Information Rights Management, 1-2
 - configuring, 8-1
 - key store, 8-2
 - SSL, 4-23
 - creating key store, 8-3
 - credential store configuration, 8-7
 - identity store configuration, 8-8
 - installing, 3-7
 - key store configuration issues, D-2
 - one-way SSL, 4-23, 4-24
 - policy store configuration, 8-7
 - postinstallation configuration, 8-1
 - Server URL configuration parameter, 8-1
 - single sign-on, 8-8
 - SSL configuration, 4-23
 - starting Managed Server, 10-4
 - validating installation, 8-8
- Oracle Internet Directory, 4-27
 - adding users, 4-35
 - reassociating identity store with, 4-27
- Oracle Inventory location, 3-9
- Oracle I/PM. *See* Oracle Imaging and Process Management
- Oracle IRM. *See* Oracle Information Rights Management
- Oracle Technology Network
 - software downloads, 1-3
 - Supported System Configurations page, 1-8
- Oracle Text 11g, patch for Oracle Database 11.1.0.7.0, 5-9
- Oracle Text Search, 5-14
 - configuration, Oracle Content Server, 5-8
 - using with Oracle URM, 9-6
- Oracle Universal Content Management, 1-1
 - configuration, 5-1
 - configuring full-text features, 7-10
 - Microsoft SQL Server configuration, 5-7
 - postinstallation configuration, 5-1
 - repository for Oracle I/PM, 7-2, 7-3, 7-7
 - Visual C++ package for Windows operating system, 4-22
- Oracle Universal Records Management, 1-2
 - configuration
 - Oracle Text Search, 9-6
 - overview, 9-1
 - Oracle Text Search, 9-6
 - postinstallation configuration, 9-1
 - search engine, Oracle Text Search, 9-6
 - setup checklist, 9-3, 9-4
- Oracle URM Adapter for Oracle UCM, installation and configuration, 5-17
- Oracle Virtual Directory, 4-27
- Oracle Web Services Manager
 - MDS schema, 4-41
 - security, 4-40
- Oracle WebLogic Server
 - creating domain, 4-3
 - domain, 1-9

- domain structure, 1-9
- extending domain, 4-10, 4-11, 4-15
- home, 1-7
- installation, 4-41
- installation module, 1-7
- installing, 3-2
- procedure for creating domain, 4-4
- starting
 - Administration Server, 10-1
 - Managed Servers, 10-2
- Oracle WSM policies
 - applying to web services, 4-43
 - securing web services with, 4-42
- Oracle WSM Policy Manager, 4-41
- Oracle WSM. *See* Oracle Web Services Manager
- outgoing provider from Oracle Content Server to Oracle IBR, 6-6
- Outside In Technology
 - libraries
 - environment variables, 4-19
 - UNIX platform, 4-19
 - Windows operating system, 4-22

P

- parameters, Java VM memory, 4-17
- passwords, key store, 8-6
- patches, Oracle Text 11g with Oracle Database 11.1.0.7.0, 5-9
- PDFExportConverter, enabling in Oracle IBR, 6-5
- policy store, configuring for Oracle IRM, 8-7
- ports
 - defaults, 4-9
 - listen ports, 4-9
 - ranges for Managed Servers, 4-9
 - SSL ports, 4-9
- postinstallation configuration
 - Oracle IBR, 6-1
 - Oracle Inbound Refinery, 6-2
 - Oracle I/PM, 7-1
 - Oracle IRM, 8-1
 - Oracle UCM, 5-1
 - Oracle Universal Records Management, 9-1
- preparing for installation, 3-1
- Prerequisite Checks screen, A-4
- project metadata, 5-14
- properties
 - InstanceDescription, 5-6
 - InstanceMenuLabel, 5-6

R

- RCU. *See* Repository Creation Utility
- reassociating identity store
 - external LDAP, 4-27
 - Oracle Internet Directory, 4-27
- rebuilding the search index, 5-16
- redeploying JSP support, 5-15
- removing Oracle home directories, 11-4
- repository

- configuring for Oracle I/PM, 7-3
- connecting Oracle I/PM to, 7-7
- Repository Creation Utility
 - creating database schemas, 1-8, 2-1
 - database
 - compatibility, 1-8
 - prerequisites, 2-1
 - dropping schemas, 11-2
 - installation module, 1-8
 - Linux operating system, 2-2
 - Select Components screen, 2-4
 - starting, 11-2
 - Windows operating system, 2-2
- restarting Managed Servers, 10-4
- roadmap, installation, 1-3
- RSA algorithm, 8-3
- run issues for Inbound Refinery, D-3

S

- schemas
 - creating, 2-1
 - dropping, 11-2, 11-3
 - Oracle Enterprise Content Management Suite, 1-4
 - Oracle WSM MDS, 4-41
 - Repository Creation Utility, 1-8
- screens
 - configuration, B-1
 - deinstallation, C-1
 - installation, A-1
- search index, 5-16
- searching, Oracle Text Search, Oracle URM, 9-6
- securing web services, 4-42
- Select a WebLogic Domain Directory screen, B-3
- Select Domain Source screen, B-4
- Select Extension Source screen, B-5
- Select JMS Distributed Destination Type screen, B-20
- Select Optional Configuration screen, B-11
- Server Socket Port, 4-41
- Server URL configuration parameter for Oracle IRM, 8-1
- setting environment variables, Outside In Technology, 4-19
- setting up a key store, 4-42
- Setup Checklist page, completing for Oracle URM, 9-3
- setup checklists, Oracle URM, 9-4
- setup issues for Inbound Refinery, D-3
- single sign-on
 - configuring for Oracle IRM, 8-8
 - Oracle Access Manager, 8-8
- Site Studio
 - configuring, 5-12
 - enabling, 5-12, 5-13
 - metadata fields, 5-14
- SiteStudioExternalApplications, 5-12
- SiteStudioExternalApplications component, 5-13

- software downloads
 - Oracle ECM, 1-2
 - Oracle E-Delivery, 1-2
 - Oracle Technology Network, 1-3
- Specify Domain Name and Location screen, B-6
- Specify Installation Location screen, A-5
- SSL
 - configuring for Oracle IRM, 4-23
 - configuring for production environment, 4-23
 - one-way, 4-23, 4-24
 - setting for development environment, 4-23, 4-24
- SSL environment, extending a domain, 4-15
- standalone applications, 5-12
 - database root CA certificate, importing into key store, 5-12
 - external database provider configuration, 5-10
 - JDBC Driver configuration, 5-10
- starting
 - Administration Server, 10-1
 - installer, 3-8
 - Managed Servers, 7-7, 10-2
 - Node Manager, 10-5
 - Oracle I/PM, 7-5, 10-2
 - Oracle IRM, 10-2
 - Repository Creation Utility, 11-2
- startup parameters, setting with Administration Console, 4-16
- stopping Oracle Fusion Middleware, 11-1
- symbolic link to chmod command, 3-8
- SysAdminAddress, 5-6
- system administrator email address, 5-6
- system configurations supported, 1-8
- System Properties Utility, 5-11
- system requirements, 3-1
- system security, resetting Oracle I/PM, 7-10

T

- Target Deployments to Clusters or Servers screen, B-18
- Target Services to Clusters or Servers screen, B-19
- Test Component Schema screen, B-10
- third-party LDAP server, 4-27
- topology, 1-10
- troubleshooting
 - additional help, D-7
 - information, D-1
 - Oracle IBR
 - conversion errors, D-6
 - login errors, D-5
 - runtime errors, D-5
 - Oracle IBR problems, D-3
 - Oracle IBR runtime errors, D-3, D-4
 - Oracle I/PM errors, connection to Oracle UCM 11g, D-3
 - tips, D-1
- TrueType fonts, 4-18

U

- UNIX operating system, fonts for National Language Support, 4-36
- UNIX platforms, libraries
 - environment variables, 4-22
 - Outside In Technology, 4-19
- USER_MEM_ARGS Environment Variable, 4-17
- users, adding, Oracle Internet Directory, 4-35

V

- verifying installation and configuration, 10-1, 10-6
- Visual C++ package for Windows operating system, 4-22

W

- web client
 - accessing, 7-5
 - Oracle I/PM, 7-7
- web layout, disabling for Oracle I/PM, 7-7
- web server name, 5-5, 6-4
- web services
 - applying Oracle WSM policies, 4-43
 - securing, 4-42
- Welcome screen
 - configuration, B-2
 - deinstallation, C-2
 - installation, A-2
- Windows Native Authentication, configuring, 4-39
- workflow server, connecting Oracle I/PM to, 7-10
- WSM. *See* Oracle Web Services Manager

Z

- zone fields, 5-14
 - full-text indexing, 5-14
 - Oracle Text Search, 5-14

