Oracle® Fusion Middleware

Installing and Configuring Oracle WebCenter Content

11*g* Release 1 (11.1.1)

E14495-14

June 2015

Oracle Fusion Middleware Installing and Configuring Oracle WebCenter Content 11*g* Release 1 (11.1.1)

E14495-14

Primary Author: Bonnie Vaughan

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

Contributors: Rob Abbe, Tom Albrecht, Satheesh Amilineni, Nathan Angstadt, Pete Chapman, Sandra Christiansen, Eric Cloney, Rupesh Das, Izeta Delic, Carl Foster, Sudhanshu Garg, Brian Gray, Helen Grembowicz, Marsha Hancock, Michael Heath, Katie Ho, MaryJo Hoepner, Mei Hong, David Jones, István Kiss , Peter LaQuerre, Bill Loi, Jeff Marshall, Ron Mellum, Liju Nair, John Neely, Saskia Nehls, Bob O'Kane-Trombley, Alejandro Paredes, Ty Paywa, Andy Peet, Ken Peterka, Wes Prichard, Rafael Ramirez, Indira Smith, Meena Srinivasan, Vani Srivastava, Gene Sutay, Matt Wall, Michael Zanchelli, Lisa Zitek-Jones

Contents

3 Configuring Oracle WebCenter Content Applications

5 Completing the Inbound Refinery Configuration

6 Completing the Imaging Configuration

12 Installing and Configuring the WebCenter Content User Interface

A Installation Screens for Oracle WebCenter Content

Preface

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

Audience

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

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

For additional information, see the following documents:

- *Oracle Fusion Middleware Administering Oracle WebCenter Content*
- *Administering Oracle WebCenter Content: Imaging*
- *Administering Oracle WebCenter Portal*
- *Administering the Application Adapters for Oracle WebCenter*
- *Administrator's Guide*
- *Administrator's Guide for Oracle Internet Directory*
- *Securing Applications with Oracle Platform Security Services*
- *Concepts*
- *Creating Domains Using the Configuration Wizard*

- *Enterprise Deployment Guide for Oracle WebCenter Content*
- *High Availability Guide*
- *Installation Guide for Oracle Identity Management*
- *Installation Guide for Oracle SOA Suite and Oracle Business Process Management Suite*
- *Installation Guide for Oracle Web Tier*
- *Installation Guide for Oracle WebLogic Server*
- *Installation Planning Guide*
- *Installing an Evaluation Instance of Oracle WebCenter Content*
- *Java EE Developer's Guide for Oracle Application Development Framework*
- *Managing Oracle WebCenter Enterprise Capture*
- *Oracle Fusion Middleware Managing Oracle WebCenter Content*
- *Node Manager Administrator's Guide for Oracle WebLogic Server*
- *Patching Guide*
- *Repository Creation Utility User's Guide*
- *Securing Oracle WebLogic Server*
- *Third-Party Application Server Guide*
- *Using Clusters for Oracle WebLogic Server*
- *Oracle Fusion Middleware Using Oracle WebCenter Content*
- *Using Oracle WebCenter Content: Desktop*
- *WebLogic Scripting Tool Command Reference*
- *Administrator and Manager's Guide for Site Studio*
- *Technical Reference Guide for Site Studio*
- *User's Guide for Site Studio Designer*

Conventions

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

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

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

1 Installation Overview

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

This chapter includes the following sections:

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

1.1 Oracle WebCenter Content Applications

Oracle WebCenter Content includes the following products:

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

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

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

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

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

  Imaging is an integrated framework of client software modules with a customizable user interface for managing documents from image capture to archiving. Client modules can be integrated within this framework to provide a single user interface, including third-party information systems, imaging, workflow process, and enterprise content management. Imaging includes the Imaging Viewer Cache and Oracle Application Extensions Framework (AXF) for BPEL.

- **Oracle WebCenter Content: AXF for BPM**

  AXF for BPM creates configurable business components, with the application development and configuration capabilities provided by technologies such as Oracle Business Process Management (Oracle BPM), Oracle Application Development Framework (Oracle ADF), Oracle Metadata Services Repository (Oracle MDS Repository), and Oracle Business Rules. Administrators can use these business components to configure and develop integration solutions for WebCenter Content business applications.

- **Oracle WebCenter Enterprise Capture (Capture)**

  Capture provides scalable document capture for centralized or distributed enterprises. It is fully integrated with Oracle WebCenter Content: Imaging and Oracle WebCenter Content to provide organizations with one system to capture, store, manage, and retrieve their mission critical business content.

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

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

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

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

After you install these products on your system, you can configure one or more of them as applications deployed to a previously installed Oracle WebLogic Server. You cannot configure an Oracle WebCenter Content 11.1.1.9.0 application in an Oracle WebLogic Server domain that already has an Oracle Enterprise Content Management Suite or Oracle WebCenter Content application from an earlier release installed.

1.2 Installation Roadmap

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

1. Perform preinstallation tasks for Oracle WebCenter Content
2. Install Oracle WebCenter Content
3. Install Other Oracle Fusion Middleware components as required
4. Configure a domain for Oracle WebCenter Content
5. Extend the Oracle WebCenter Content domain as required
6. Perform Postinstallation Configuration
7. Verify the Configuration

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

Figure 1–1 Roadmap for Installing and Configuring Oracle WebCenter Content

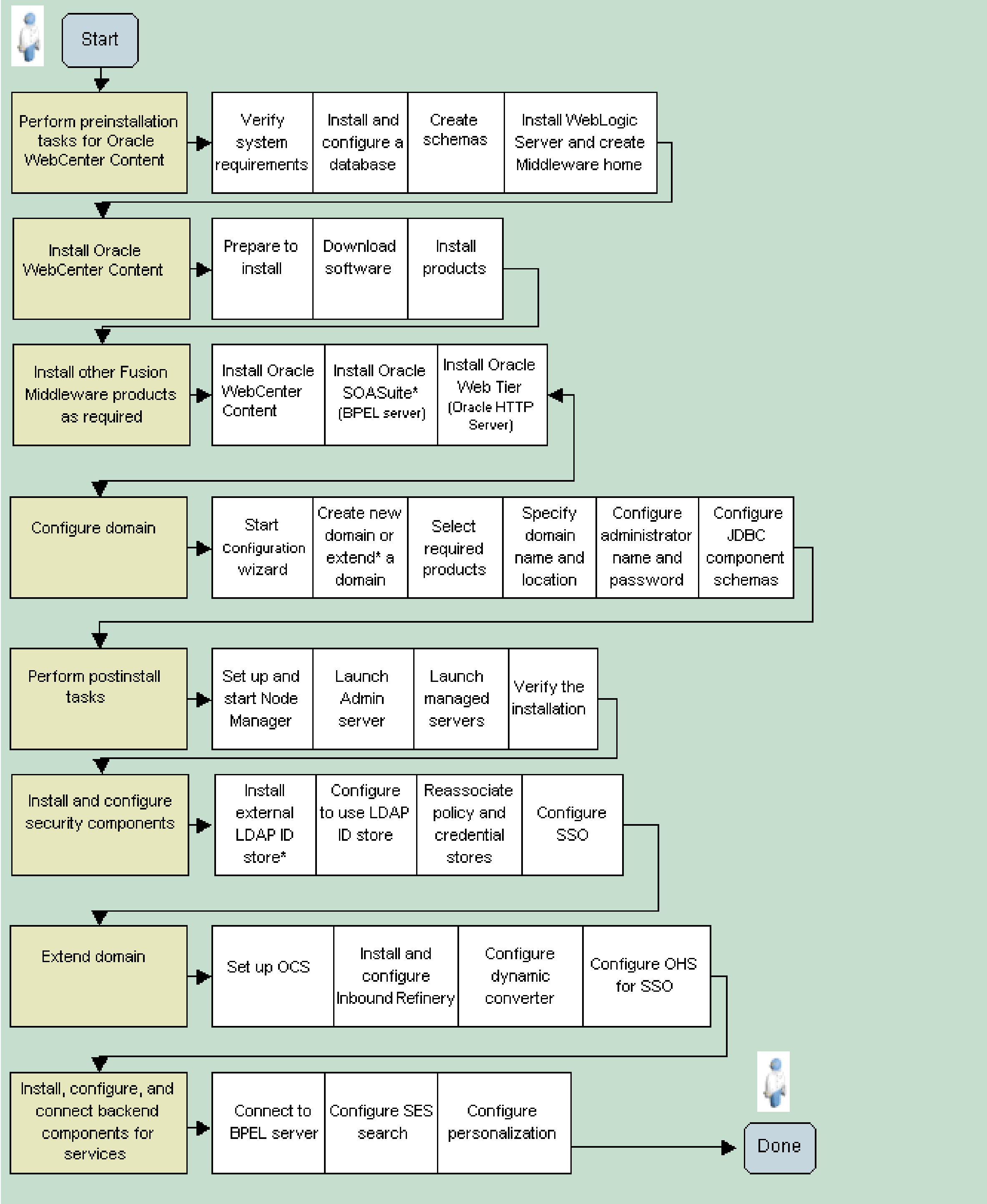

Start
Perform preinstallation tasks for Oracle WebCenter Content
Verify system requirements
Install and configure a database
Create schemas
Install WebLogic Server and create Middleware home
Install Oracle WebCenter Content
Prepare to install
Download software
Install products
Install other Fusion Middleware products as required
Install Oracle WebCenter Content
Install Oracle SOASuite* (BPEL server)
Install Oracle Web Tier (Oracle HTTP Server)
Configure domain
Start Configuration wizard
Create new domain or extend* a domain
Select required products
Specify domain name and location
Configure administrator name and password
Configure JDBC component schemas
Perform postinstall tasks
Set up and start Node Manager
Launch Admin server
Launch managed servers
Verify the installation
Install and configure security components
Install external LDAP ID store*
Configure to use LDAP ID store
Reassociate policy and credential stores
Configure SSO
Extend domain
Set up OCS
Install and configure Inbound Refinery
Configure dynamic converter
Configure OHS for SSO
Install, configure, and connect backend components for services
Connect to BPEL server
Configure SES search
Configure personalization
Done

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

If you are going to configure Oracle WebCenter Content: AXF for BPM or Oracle Application Extensions Framework for BPEL (AXF for BPEL), follow the roadmap in Table 1–2.

Table 1–1 Oracle WebCenter Content Installation Procedure

Task	Description	Required	Optional
1. Preparing for installation	Ensure that your system environment meets the general installation requirements for Oracle Fusion Middleware, for Oracle WebCenter Content, and for the Repository Creation Utility (RCU), which requires a supported database.	Section 2.1, "Preparing to Install."	
2. Creating schemas for applications	Oracle WebCenter Content applications require schemas that must be installed in a supported database, such as Oracle Database, Microsoft SQL Server, or IBM DB2. Prepare a database for Oracle WebCenter Content schemas, then install RCU and use it to create schemas. **Note:** You can perform this task before or after task 3, "Installing an application server and Oracle Fusion Middleware" and task 4, "Installing Oracle WebCenter Content."	Section 2.2, "Creating Oracle WebCenter Content Schemas with the Repository Creation Utility"	
3. Installing an application server and Oracle Fusion Middleware	Oracle WebCenter Content runs on Oracle WebLogic Server. You must install Oracle WebLogic Server, or a supported third-party application server, before you install Oracle WebCenter Content. The Oracle WebLogic Server Installer creates the Oracle WebLogic Server home directory (*WL_HOME*) within the Middleware home directory (*MW_HOME*). **Note:** You can perform this task before or after task 2, "Creating schemas for applications."	Section 2.3, "Installing an Application Server and Oracle Fusion Middleware"	
4. Installing Oracle WebCenter Content	Use the Oracle Fusion Middleware 11*g* WebCenter Content Installer to install Oracle WebCenter Content. The installer creates an Oracle home directory where it installs the Oracle WebCenter Content products. The installer lays down the Oracle WebCenter Content binaries for these products: ■ WebCenter Content ■ Inbound Refinery ■ Imaging ■ AXF for BPM ■ Oracle WebCenter Enterprise Capture ■ Oracle IRM ■ Records **Note:** You can perform this task before or after task 2, "Creating schemas for applications," but you need to perform it after task 3, "Installing an application server and Oracle Fusion Middleware."	Section 2.4, "Using the Installer for Oracle WebCenter Content"	

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

Task	Description	Required	Optional
5. Configuring Oracle WebCenter Content	Create or extend an Oracle WebLogic Server domain and choose the products that you want to deploy and configure as applications. The Fusion Middleware Configuration Wizard creates an Oracle WebLogic Server domain, which contains the Administration Server and one or more Managed Servers, depending on the products that you choose. After you have created a domain, you can later extend that domain to deploy and configure additional Oracle WebCenter Content products as applications.	Chapter 3, "Configuring Oracle WebCenter Content Applications"	
6. Installing and configuring an external LDAP-based identity store	By default, Oracle WebCenter Content uses the Oracle WebLogic Server embedded LDAP server. Although secure, the out-of-the-box embedded LDAP may not scale appropriately for enterprise production environments. In a production system, Oracle WebCenter Content applications need to use an external Lightweight Directory Application Protocol (LDAP) authentication provider rather than the Oracle WebLogic Server embedded LDAP server. To manage the identities of users across diverse servers and enable single sign-on across applications, you must install and configure an external LDAP-based identity store. **Note:** If you perform this task before task 7, "Performing Postinstallation Configuration" and task 8, "Verifying the Configuration," the postinstallation configuration is easier.	Section 3.9, "Reassociating the Identity Store with an External LDAP Authentication Provider" for Oracle WebLogic Server in Production mode or IBM WebSphere Application Server.	Section 3.9, "Reassociating the Identity Store with an External LDAP Authentication Provider" for Oracle WebLogic Server in Development mode.
7. Performing Postinstallation Configuration	For each Oracle WebCenter Content application, you need to perform some initial configuration to get the application up and running in the Managed Server. Some of this initial configuration needs to be done before you start the Managed Server for the first time.	Chapter 4, "Completing the WebCenter Content Configuration" Chapter 5, "Completing the Inbound Refinery Configuration" Chapter 6, "Completing the Imaging Configuration" Chapter 9, "Completing the Oracle IRM Configuration" Chapter 8, "Completing the Records Configuration"	

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

Task	Description	Required	Optional
8. Verifying the Configuration	To verify the installation, you can start the Administration Server and Managed Servers. Before you can start a Managed Server the first time, you must start the Administration Server. To start working with an Oracle WebCenter Content application, you must start the Managed Server to which that application is deployed. You can then access the application's URL and complete the configuration according to your requirements.	Chapter 10, "Verifying the Oracle WebCenter Content Configuration"	

Table 1–2 shows the roadmap for installing AXF for BPM and AXF for BPEL.

Table 1–2 Oracle WebCenter Content Installation Procedure for AXF for BPM and AXF for BPEL

Task	Description	Required	Optional
1. Preparing for installation	Ensure that your system environment meets the general installation requirements for Oracle Fusion Middleware, for Oracle WebCenter Content, and for the Repository Creation Utility (RCU), which requires a supported database.	Section 2.1, "Preparing to Install."	
2. Creating schemas for applications	Oracle WebCenter Content applications require schemas that must be installed in a supported database, such as Oracle Database, Microsoft SQL Server, or IBM DB2. Prepare a database for Oracle WebCenter Content schemas, then install RCU and use it to create schemas.	Section 2.2, "Creating Oracle WebCenter Content Schemas with the Repository Creation Utility"	
3. Installing an application server and Oracle Fusion Middleware	Oracle WebCenter Content runs on Oracle WebLogic Server. You must install Oracle WebLogic Server, or a supported third-party application server, before you install Oracle WebCenter Content. The Oracle WebLogic Server Installer creates the Oracle WebLogic Server home directory (*WL_HOME*) within the Middleware home directory (*MW_HOME*).	Section 2.3, "Installing an Application Server and Oracle Fusion Middleware"	
4. Installing Oracle SOA Suite	The installer creates an Oracle home directory where it installs Oracle SOA Suite. If you are installing Oracle SOA Suite in the same domain as the AXF for BPM or AXF for BPEL product, follow the Single Domain directions; otherwise, proceed to the Multidomain/Multimachine: directions, as outlined in the following rows.		
	4a. Single Domain	Note in `Section 2.4` to install Oracle SOA Suite	

Table 1–2 (Cont.) Oracle WebCenter Content Installation Procedure for AXF for BPM and AXF for BPEL

Task	Description	Required	Optional
	4b. Multidomain/Multimachine: Oracle SOA Suite and Imaging run on Oracle WebLogic Server. You must install Oracle WebLogic Server, or a supported third-party application server, before you install Oracle SOA Suite.	Section 2.2, "Creating Oracle WebCenter Content Schemas with the Repository Creation Utility" Section 2.3, "Installing an Application Server and Oracle Fusion Middleware" Note in `Section 2.4` to install Oracle SOA Suite	
5. Installing Oracle WebCenter Content	Use the Oracle Fusion Middleware 11*g* WebCenter Content Installer to install Oracle WebCenter Content. The installer creates an Oracle home directory where it installs the Oracle WebCenter Content products. The installer lays down the Oracle WebCenter Content binaries for these products: ■ WebCenter Content ■ Inbound Refinery ■ Imaging, which includes AXF for BPEL ■ AXF for BPM ■ Oracle WebCenter Enterprise Capture ■ Oracle IRM ■ Records	Section 2.4, "Using the Installer for Oracle WebCenter Content"	
6. Configuring Oracle WebCenter Content	Create or extend an Oracle WebLogic Server domain and choose the products that you want to deploy and configure as applications. The Fusion Middleware Configuration Wizard creates an Oracle WebLogic Server domain, which contains the Administration Server and one or more Managed Servers, such as `IPM_server1`, depending on the products that you choose. After you have created a domain, you can later extend that domain to deploy and configure additional Oracle WebCenter Content products as applications.	Section 3.2, "Creating an Oracle WebLogic Server Domain" Section 3.5, "Increasing the Java VM Heap Size for Managed Servers" Section 3.6, "Setting Up Fonts on a UNIX System"	
7. Installing and configuring an external LDAP-based identity store	If you are installing Oracle SOA Suite onto the same domain as the AXF for BPM or AXF for BPEL product you can follow the instructions for either Single Domain or Multidomain/Multimachine in the following rows; otherwise; proceed to the Multidomain/Multimachine instructions.		

Table 1–2 (Cont.) Oracle WebCenter Content Installation Procedure for AXF for BPM and AXF for BPEL

Task	Description	Required	Optional
	7a. Single Domain: By default, Oracle WebCenter Content uses the Oracle WebLogic Server embedded LDAP server. Although secure, the out-of-the-box embedded LDAP may not scale appropriately for enterprise production environments.		Section 3.8, "Configuring SSL for Oracle WebCenter Content Applications" Section 3.9, "Reassociating the Identity Store with an External LDAP Authentication Provider"
	7b. Multidomain/Multimachine: In a production system, Oracle WebCenter Content applications need to use an external Lightweight Directory Application Protocol (LDAP) authentication provider rather than the Oracle WebLogic Server embedded LDAP server. To manage the identities of users across diverse servers and enable single sign-on across applications, you must install and configure an external LDAP-based identity store.	Section 3.9, "Reassociating the Identity Store with an External LDAP Authentication Provider" For information, see "Enabling Trust Between WebLogic Server Domains" in *Oracle Fusion Middleware Securing Oracle WebLogic Server*.	Section 3.8, "Configuring SSL for Oracle WebCenter Content Applications"
8. Performing Postinstallation Configuration	For each Oracle WebCenter Content application, you need to perform some initial configuration to get the application up and running in the Managed Server. Some of this initial configuration needs to be done before you start the Managed Server for the first time.	Section 6.5.1.1, "Configuring AXF for BPM"	Section 6.2, "Configuring the Full-Text Features in the WebCenter Content Repository" Section 6.4, "Configuring the Imaging Viewer Cache" Chapter 7, "Completing the Oracle WebCenter Enterprise Capture Configuration"
9. Verifying the Configuration	To verify the installation, you need to start the Administration Server and Managed Servers.	Section 6.5.1.2, "Verifying the AXF for BPM Installation"	Section 6.5.2.3, "Verifying the AXF for BPEL Installation and Configuration with HelloBpel"

1.2.1 Installation Modules

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

- Oracle Fusion Middleware and Oracle WebLogic Server Homes
- Database
- Repository Creation Utility
- Oracle WebCenter Content
- Oracle SOA Suite (for AXF and Imaging)

1.2.1.1 Oracle Fusion Middleware and Oracle WebLogic Server Homes

Oracle WebCenter Content requires a Middleware home and an application server on your system. If your system does not already have Oracle WebLogic Server, you can install it in a new Middleware home directory, as described in Section 2.3, "Installing an Application Server and Oracle Fusion Middleware."

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

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

```
/middleware_home
     coherence_3.7
     logs
     modules
     wlserver_10.3
     oracle_common
     utils
     WCC_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). *MW_HOME* represents the location of a Middleware home in path names. For more information, see "Middleware Home and WebLogic Home Directories" in the *Installation Planning Guide*.

The WebCenter Content Oracle home contains the binary and library files necessary for Oracle WebCenter Content. *WCC_ORACLE_HOME* represents the WebCenter Content Oracle home in path names. The default WebCenter Content Oracle home is *MW_HOME*/Oracle_ECM1 on a UNIX operating system or *MW_HOME*\Oracle_ECM1 on a Windows operating system. The WebCenter Content Oracle home can be associated with multiple Oracle WebLogic Server domains. The Oracle Common home contains the binary and library files required for Oracle Enterprise Manager Fusion Middleware Control and Java Required Files (JRF).

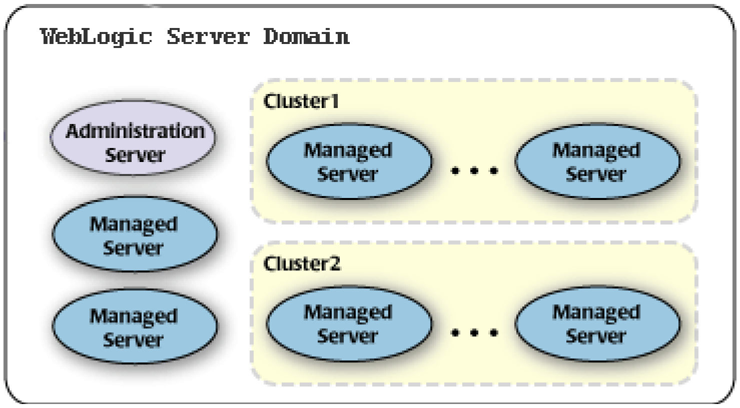
For more information about the structure and contents of a Middleware home, see "Understanding Oracle Fusion Middleware Concepts" in the *Administrator's Guide*.

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

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

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

Figure 1–2 Oracle WebLogic Server Domain Structure



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

1.2.1.2 Database

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

The overall performance of a WebCenter Content system is dependent on the speed at which files that are checked into the server can be stored and retrieved. Using a database to store the files that are stored in the server requires that the database can execute both Read and Write commands at speeds similar to a file system. Oracle WebCenter Content with Oracle Database 11*g* meets this standard because it uses Oracle Secure Files to store content items. For databases other than Oracle Database, consult your database provider to ensure that the database can achieve your storage and retrieval requirements.

For more information, see Section 2.1.5, "Installing and Configuring a Supported Database."

1.2.1.3 Repository Creation Utility

You need to install and run Repository Creation Utility (RCU) to create database schemas for Oracle WebCenter Content applications that you plan to configure.

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

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

1.2.1.4 Oracle WebCenter Content

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

1.2.1.5 Oracle SOA Suite (for AXF and Imaging)

AXF for BPM and AXF for BPEL need Oracle SOA Suite installed, in the same domain as Oracle WebCenter Content or in a separate domain. Imaging usually requires Oracle SOA Suite as well. You can install Oracle SOA Suite on the same machine as the Oracle WebCenter Content applications or on a different machine.

1.2.2 Software Downloads for Oracle WebCenter Content Installation and Configuration

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

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

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

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

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

1. Go to the Oracle Software Delivery Cloud website 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 Oracle Fusion Middleware 11*g*, which includes Oracle WebCenter Content.
6. Click the **Description** link to display a list of downloadable ZIP files for the media pack.

   Each ZIP file has a unique part number.

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

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

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

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

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

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

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

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

   `http://www.oracle.com/technetwork/database/enterprise-edition/downloads/index.html`

   Download Oracle Database 11*g* for your platform.

   Instead of Oracle Database, you can use Microsoft SQL Server or IBM DB2. For information about database versions supported by Repository Creation Utility and Oracle WebCenter Content, see the Oracle Fusion Middleware Supported System Configurations page on Oracle Technology Network at

   `http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html`

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

   `http://www.oracle.com/technetwork/middleware/fusion-middleware/downloads/index.html`

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

   - **SOA Suite (11.1.1.9.0)** under Runtime Software
   - **JDeveloper and Application Development Framework (11.1.1.9.0)** under Required Additional Software

     After JDeveloper is installed, you must install the Oracle SOA Suite Design-Time Components. Oracle SOA Suite is not automatically installed with JDeveloper. Before you can create a SOA application and project, you must install the Oracle SOA Suite Extension for JDeveloper. For information about installing and configuring Oracle SOA Suite, see the *Oracle Fusion Middleware Installation Guide for Oracle SOA Suite and Oracle Business Process Management Suite*.

1.3 Topology Summary for Oracle WebCenter Content

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

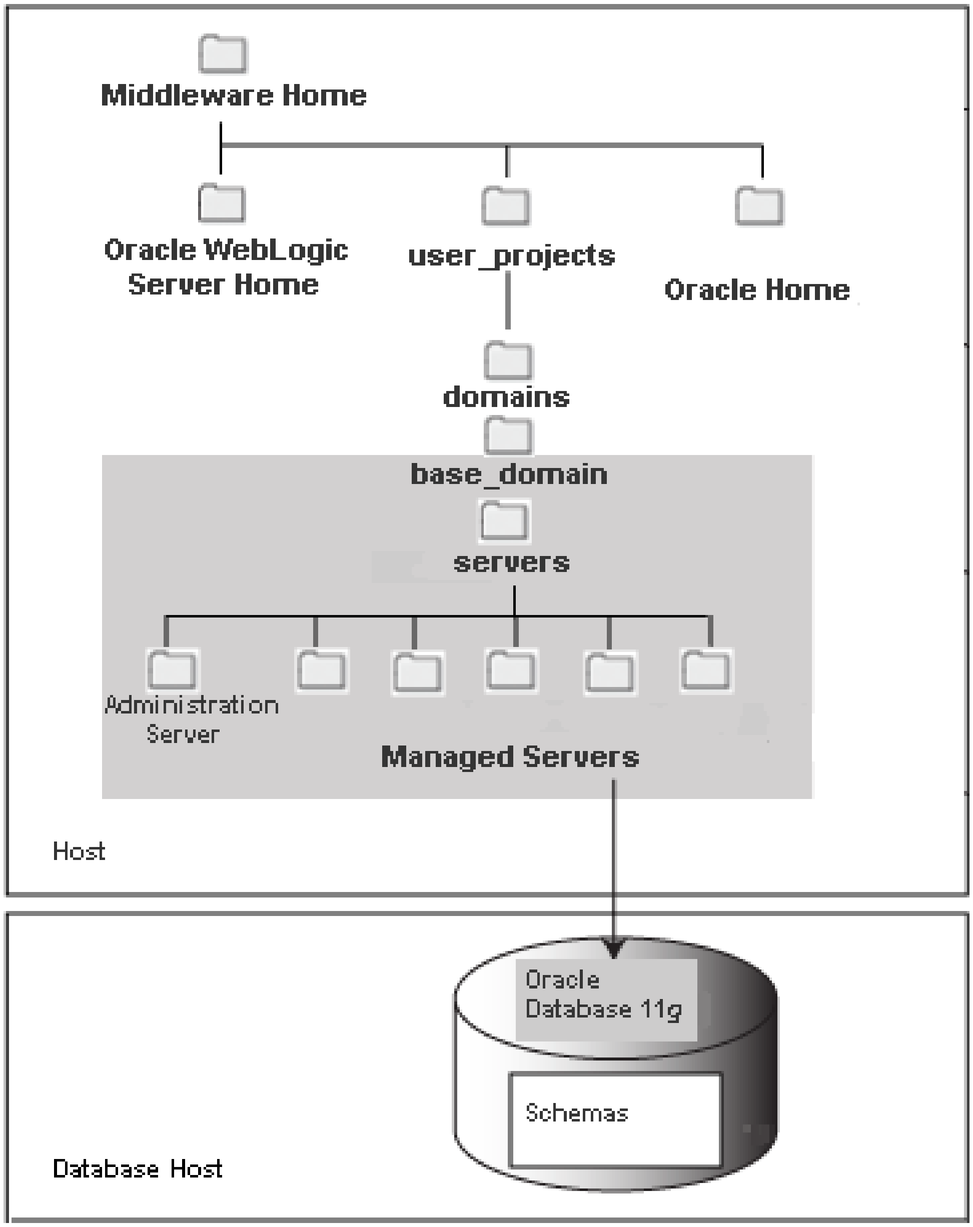
When you install Oracle WebCenter Content, a WebCenter Content Oracle home directory (*WCC_ORACLE HOME*) is created under the Middleware home directory. The WebCenter Content Oracle home directory contains the binary and library files for Oracle WebCenter Content.

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

- WebCenter Content Managed Server
- Inbound Refinery Managed Server
- Imaging Managed Server
- Oracle WebCenter Enterprise Capture Managed Server
- Oracle IRM Managed Server
- Records Managed Server

Figure 1–3 illustrates the directory structure that installation and configuration of these products will create on your system.

Figure 1–3 Directory Structure of an Oracle WebCenter Content Installation



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

2 Installing Oracle WebCenter Content

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

This chapter includes the following sections:

2.1 Preparing to Install

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

To provide accessibility on a Windows operating system, you can also install Java Access Bridge. For more information, see "Installing and Configuring Java Access Bridge" in the *Oracle Java Access Bridge Installation and Application Developer's Guide* at

`http://docs.oracle.com/javase/accessbridge/2.0.2/toc.htm`

For information about libraries and environment variables that you need, see Section 3.7, "Installing Libraries and Setting Environment Variables."

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

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

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

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

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

   ```
   HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control/FileSystem
   ```

2. Set the value of the `NtfsDisable8dot3NameCreation` key to 1.
3. Restart the Windows operating system for the change to take effect.

2.1.2 Enabling Unicode Support

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

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

You can verify that the `LANG` and `LC_ALL` environment variables are set by typing the following two commands on a UNIX operating system:

- `echo $LANG`
- `echo $LC_ALL`

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

2.1.3 Reviewing System Requirements and Certification

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

- Oracle Fusion Middleware System Requirements and Specifications page at

  `http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-requirements-100147.html`

  The "Oracle Fusion Middleware System Requirements and Specifications" document for 11*g* Release 1 (11.1.1) 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 page at

  `http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html`

  The System Requirements and Supported Platforms for Oracle WebCenter Content 11gR1 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, unless you are instructed to do so.
- For a 64-bit Linux operating system, you should use the 32-bit Java Runtime Environment (JRE) on a client machine for the Imaging Advanced Viewer.
- If you are using the IBM JDK with Oracle WebCenter Content and an IBM WebSphere Application Server version earlier than 7.0.0.27, certain functionality, such as the check for patches feature, will not work correctly unless the Java socket factories are changed. The IBM JRE has its own Secure Sockets Layer (SSL) socket factories. For more information, see "Changing Java Socket Factories in the IBM JDK" in the *Third-Party Application Server Guide*.
- For Oracle Linux 6.4, you need the following packages installed on the operating system so it can detect the Oracle Universal Installer for Oracle WebCenter Content 11*g* (11.1.1.6.0) or later:

```
redhat-lsb-graphics-4.0-7.0.1.el6.x86_64
redhat-lsb-compat-4.0-7.0.1.el6.x86_64
redhat-lsb-core-4.0-7.0.1.el6.x86_64
redhat-lsb-printing-4.0-7.0.1.el6.x86_64
redhat-lsb-4.0-7.0.1.el6.x86_64
```

2.1.4 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**.

2.1.5 Installing and Configuring a Supported Database

The database that you use for Oracle WebCenter Content applications must be compatible with Repository Creation Utility (RCU), which creates the schemas for the Oracle WebCenter Content applications.

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

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

http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html

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

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

2.2 Creating Oracle WebCenter Content Schemas with the Repository Creation Utility

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

- Preparing to Run RCU and Load Schemas
- Creating Schemas for Oracle WebCenter Content Applications

2.2.1 Preparing to Run RCU and Load Schemas

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

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

2.2.1.1 Database Prerequisites

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

Oracle Database 11*g* is required for using Oracle WebCenter Enterprise Capture because Capture uses Oracle Platform Security Services (OPSS), which works only with Oracle Database for its schema.

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

http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.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/technetwork/middleware/ias/downloads/fusion-requirements-100147.html

2.2.1.2 Database Maintenance for Oracle WebCenter Content Schemas

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

2.2.1.3 RCU for Linux and Windows Operating Systems

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

2.2.2 Creating Schemas for Oracle WebCenter Content Applications

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

- Oracle WebCenter Content (WebCenter Content, which includes Oracle WebCenter Content Server)
- Oracle WebCenter Content: Imaging
- Oracle WebCenter Enterprise Capture
- Oracle Information Rights Management (Oracle IRM)
- Oracle WebCenter Content: Records
- Oracle WebCenter Content Server - Search

You can download a ZIP file containing the Repository Creation Utility from either of the following websites:

- Oracle Software Delivery Cloud at

  http://edelivery.oracle.com/

- Oracle Fusion Middleware 11*g* Software Downloads page (WebCenter Content link) on Oracle Technology Network (OTN) at

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

After downloading the ZIP file, you can extract the contents to a directory of your choice.

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

To create schemas for Oracle WebCenter Content applications:

1. Unzip the ZIP file containing the Repository Creation Utility to a location, *media_loc*, and then start RCU:

   - **UNIX path:** *media_loc*/*RCU_HOME*/bin/rcu
   - **Windows path:** *media_loc*\RCU_HOME\bin\rcu.bat

2. Welcome screen

   Click **Next**.

3. Create Repository screen

   Select **Create**.

   Click **Next**.

4. Database Connection Details screen

   Database Type: Select one of these types:

   - **Oracle Database** (the default type)
   - **Oracle Database enabled for edition-based redefinition**
   - **Microsoft SQL Server**
   - **IBM DB2**

   > **For SQL Server:** Before you can use SQL Server with WebCenter Content, you need to turn on snapshot isolation in the database. If you plan to use SQL Server for the back-end database for Imaging and Oracle SOA Suite, you also need to configure the Metadata Services (MDS) repository in the database and then create an MDS schema on the Select Components screen (Step 5).
   >
   > The prerequisite configurations for WebCenter Content and the MDS repository follow:
   >
   > 1. Log in to the database with a user name that has DBA privileges and does not have multiple logins to the database.
   >
   >   Multiple logins for the DBA would result in a lock error.
   >
   > 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 IBM DB2:** Before you create a schema in an IBM DB2 database, you need to manually set DatabasePreserveCase=1 in the *DomainHome*/ucm/cs/config/config.cfg file.

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

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

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

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

- **Port:** Specify the database listen port number. The default port number is `1521` for an Oracle Database instance, `1433` for Microsoft SQL Server, or `50000` for IBM DB2.

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

  If you do not know the service name for your database, you can obtain it from the `SERVICE_NAMES` parameter in the database's initialization parameter file. If this file does not contain the `SERVICE_NAMES` parameter, then the service name is the same as the global database name, which is specified in the `DB_NAME` and `DB_DOMAIN` parameters. Another way to find the service name is to log in to the database as `SYS` and run the following command:

  ```
  show parameter service_name
  ```

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

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

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

  For Microsoft SQL Server, specify the name of a user with SYSDBA or DBA privileges.

  For IBM DB2, RCU needs to connect as the MDS schema owner. Specify an operating system user for the MDS database schema (for example, `OWSM_MDS`). An operating system user has to be created before you use RCU to create an MDS schema in an IBM DB2 database.

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

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

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

  `SYS` requires the SYSDBA role.

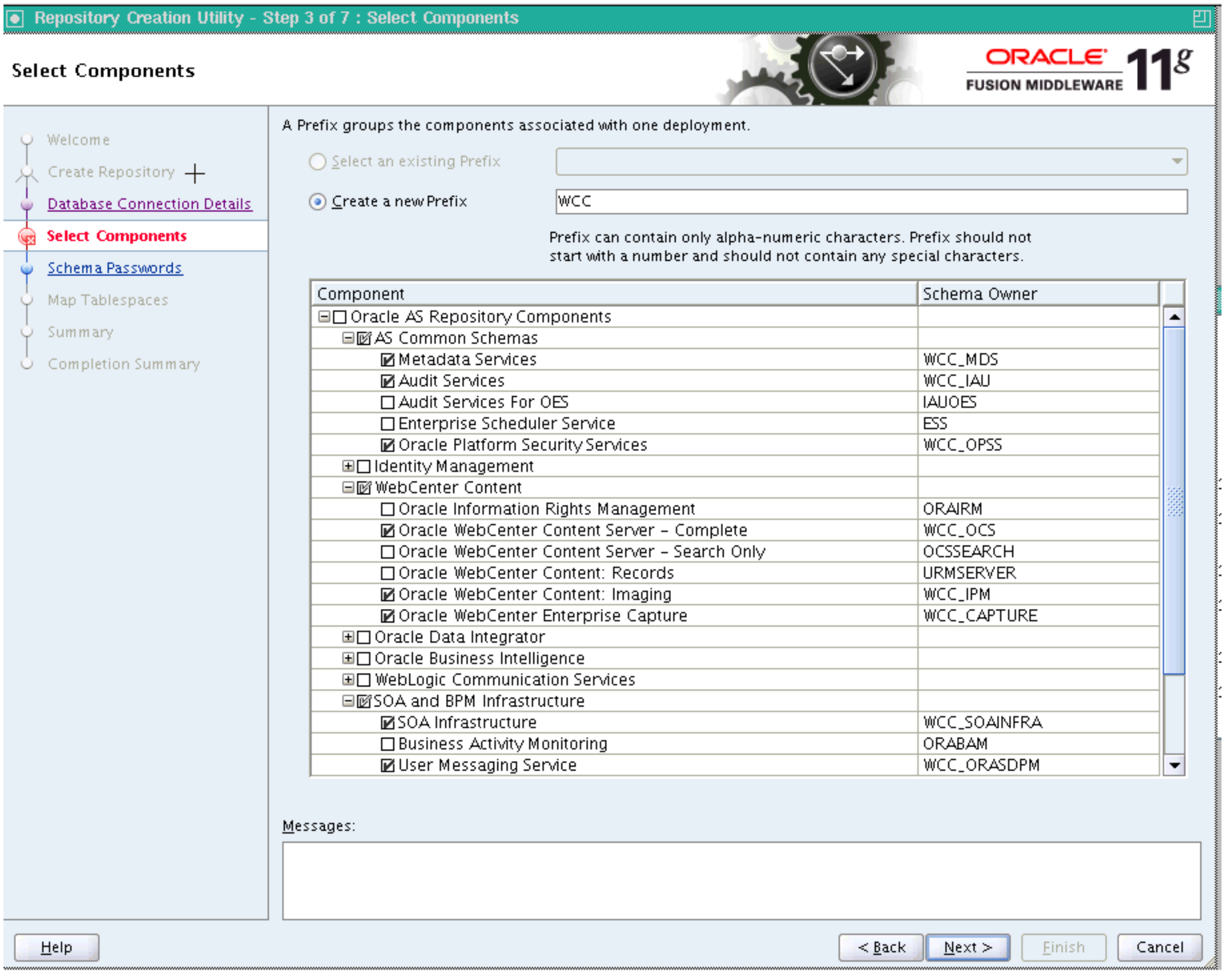
Click **Next**. The Checking Global Prerequisites dialog box appears.

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

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

5. Select Components screen

Figure 2–1 RCU Select Components Screen



A Prefix groups the components associated with one deployment.

○ Select an existing Prefix

● Create a new Prefix: WCC

Prefix can contain only alpha-numeric characters. Prefix should not start with a number and should not contain any special characters.

Component	Schema Owner
⊟ □ Oracle AS Repository Components	
⊟ ☑ AS Common Schemas	
☑ Metadata Services	WCC_MDS
☑ Audit Services	WCC_IAU
□ Audit Services For OES	IAUOES
□ Enterprise Scheduler Service	ESS
☑ Oracle Platform Security Services	WCC_OPSS
⊞ □ Identity Management	
⊟ ☑ WebCenter Content	
□ Oracle Information Rights Management	ORAIRM
☑ Oracle WebCenter Content Server - Complete	WCC_OCS
□ Oracle WebCenter Content Server - Search Only	OCSSEARCH
□ Oracle WebCenter Content: Records	URMSERVER
☑ Oracle WebCenter Content: Imaging	WCC_IPM
☑ Oracle WebCenter Enterprise Capture	WCC_CAPTURE
⊞ □ Oracle Data Integrator	
⊞ □ Oracle Business Intelligence	
⊞ □ WebLogic Communication Services	
⊟ ☑ SOA and BPM Infrastructure	
☑ SOA Infrastructure	WCC_SOAINFRA
□ Business Activity Monitoring	ORABAM
☑ User Messaging Service	WCC_ORASDPM

Messages:

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_CAPTURE could be DEV_ODC, DEV_URMSERVER could be DEV_URM, and DEV_ORAIRM could be DEV_IRM.

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

- **Oracle Information Rights Management**
- **Oracle WebCenter Content Server - Complete**

  (for WebCenter Content)
- **Oracle WebCenter Content Server - Search Only**

- **Oracle WebCenter Content: Records**
- **Oracle WebCenter Content: Imaging**
- **Oracle WebCenter Enterprise Capture**

To create a schema for WebCenter Content:

- Select **Oracle WebCenter Content Server - Complete**.

To create an OCSSEARCH schema for OracleTextSearch:

- For an external data source or for IBM DB2 database searches, select **Oracle WebCenter Content Server - Search Only**. For more information, see Section 4.3.2, "Configuring the Content Server Instance," and Section 4.5, "Configuring OracleTextSearch for Content Server."

To create schemas for Imaging:

- Select **Oracle WebCenter Content: Imaging**, and also select **Oracle WebCenter Content Server - Complete** to use WebCenter Content as the Imaging repository.
- For Oracle Web Services Manager (Oracle WSM) Policy Manager, or for using Imaging with Oracle SOA Suite, expand **AS Common Schemas** and select **Metadata Services**. If you are using Microsoft SQL Server for the back-end database, you need to configure MDS as described in Step 4 before you select **Metadata Services** on this screen.

To create schemas for AXF for BPM:

- Select **WebCenter Content > Oracle WebCenter Content: Imaging**.
- If you are going to use AXF for BPM with Imaging, you also need schemas for the following components:
  - **WebCenter Content > Oracle WebCenter Content Server - Complete**
  - **AS Common Schemas > Metadata Services**
  - **SOA and BPM Infrastructure > SOA Infrastructure**
  - **SOA and BPM Infrastructure > User Messaging Service** (automatically created with the **SOA Infrastructure** schema)
  - **Identity Management > Oracle Internet Directory** (automatically created)

To create schemas for Oracle WebCenter Enterprise Capture:

- Select **Oracle WebCenter Enterprise Capture**.
- You also need schemas for the following components, which are automatically selected under **AS Common Schemas** when you select **Oracle WebCenter Enterprise Capture** because Capture uses the MDS and OPSS schemas:
  - **Metadata Services** (automatically created with the Imaging schema)
  - **Oracle Platform Security Services**

    Oracle Platform Security Services (OPSS) works only with Oracle Database 11*g* for its schema, but the OPSS schema is necessary for a Cluster setup (unless you are using Oracle Internet Directory and are going to reassociate the security store using it).

Either Oracle Internet Directory or an OPSS schema is necessary for a Capture cluster because the `system-jazn-data.xml` file is not sufficient for a cluster setup. If the security store is not in either Oracle Internet Directory or the OPSS schema in the database, the two nodes get out of sync because the `system-jazn-data.xml` file on the second node in the cluster gets overwritten, as Node Manager will sync the data from first node and overwrite the file on second node. With the OPSS schema or Oracle Internet Directory, the application data is preserved in a shared location to which both nodes have access.

If you use OPSS, a data source for it must be created manually after the domain is created.

To create a schema for the WebCenter Content user interface:

- Select **Metadata Services**.

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

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 a password in the **Schema Password** and **Confirm Password** columns.

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

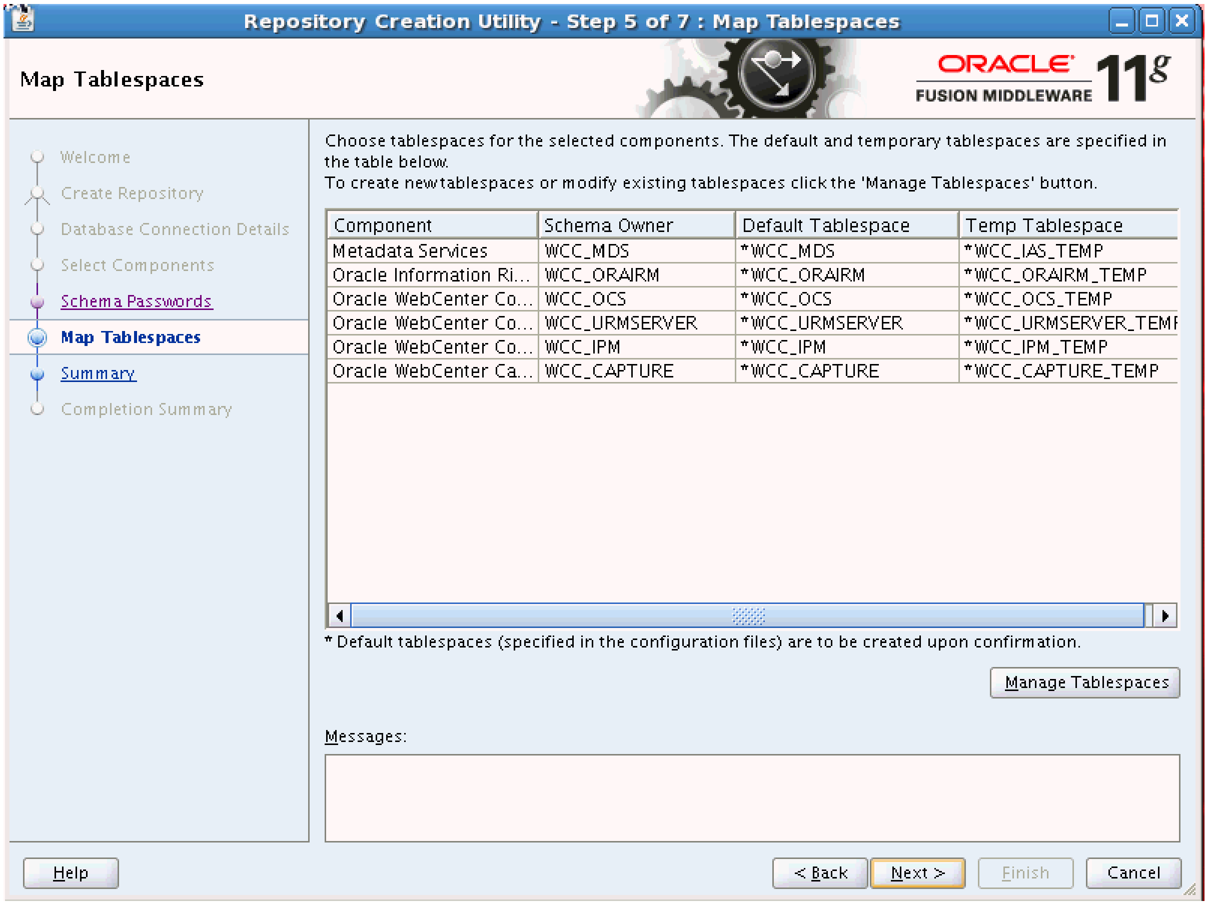
   Note: Record all schema passwords from this screen because you will need them later to configure your applications.

   Click **Next**.

7. Map Tablespaces screen

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

Figure 2–2 Default Oracle WebCenter Content Tablespaces on Map Tablespaces Screen



Choose tablespaces for the selected components. The default and temporary tablespaces are specified in the table below.
To create new tablespaces or modify existing tablespaces click the 'Manage Tablespaces' button.

Component	Schema Owner	Default Tablespace	Temp Tablespace
Metadata Services	WCC_MDS	*WCC_MDS	*WCC_IAS_TEMP
Oracle Information Ri...	WCC_ORAIRM	*WCC_ORAIRM	*WCC_ORAIRM_TEMP
Oracle WebCenter Co...	WCC_OCS	*WCC_OCS	*WCC_OCS_TEMP
Oracle WebCenter Co...	WCC_URMSERVER	*WCC_URMSERVER	*WCC_URMSERVER_TEMI
Oracle WebCenter Co...	WCC_IPM	*WCC_IPM	*WCC_IPM_TEMP
Oracle WebCenter Ca...	WCC_CAPTURE	*WCC_CAPTURE	*WCC_CAPTURE_TEMP

* Default tablespaces (specified in the configuration files) are to be created upon confirmation.

If you want to create new tablespaces or modify or remove existing ones, click **Manage Tablespaces**, and go to the next step.

To validate the tablespaces, click **Next** on the Map Tablespaces screen. The Confirmation dialog box appears. Click **OK** to create tablespaces. 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:

- Record each schema owner name from this screen because you will need it later, in the format *schemaprefix_schemasuffix*, to configure the corresponding application.

  For example, if you used the default prefix, DEV_, you would supply the following owner name for the Records schema in Oracle Database:

  ```
  DEV_URMSERVER
  ```

  For IBM DB2, however, the schema owner name is limited to 8 characters, with up to 4 characters for the prefix. If the default name of the schema suffix is longer than 3 characters, you need to change it for IBM DB2 on the Configure JDBC Component Schema screen. For example, DEV_CAPTURE could be DEV_ODC, DEV_URMSERVER could be DEV_URM, and DEV_ORAIRM could be DEV_IRM.

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

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

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

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

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

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

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

8. Manage Tablespaces screen

   You can go to the next step if you are not managing any tablespaces.

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

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

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

To remove a tablespace:

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

b. Click **Remove**.

   This tablespace will not get created.

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

To modify or add a tablespace:

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

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

c. Specify the values you want in these fields:

   * **Name**

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

   * **Type**

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

   * **Block Size (KB)**

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

   * **Storage Type**

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

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

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

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

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

   * **File Name**

     Specify the name of the data file.

   * **File Directory**

     Specify the location where this data file will reside.

   * **Size**

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

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

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

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

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

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

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

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

9. Summary screen

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

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

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

10. Completion Summary screen

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

    Click **Close**.

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

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

2.3 Installing an Application Server and Oracle Fusion Middleware

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

To install Oracle WebLogic Server in a Middleware home:

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

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

   The 32-bit and 64-bit executable files from which you can install Oracle WebLogic Server are bundled with the appropriate JDK version. If you use the JAR files, 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/technetwork/middleware/ias/downloads/fusion-certification-100350.html`

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

   - **Invoke Using UNIX BINs**

     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.

     In the following commands, `wls103`*n* can be either `wls1035` or `wls1036`.

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

     ```
     ./wls103n_linux32.bin
     ```

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

     ```
     ./wls103n_linux64.bin
     ```

   - **Invoke Using UNIX JARs**

     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.

In the following commands, `wls103n` can be either `wls1035` or `wls1036`.

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 wls103n_generic.jar

JAVA_HOME/bin/java -d64 -jar wls103n_generic.jar
```

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
```

- **Invoke Using a Windows System**

  In the following commands, `wls103n` can be either `wls1035` or `wls1036`.

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

  ```
  wls103n_win32.exe
  ```

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

  ```
  JAVA_HOME\bin\java -jar wls103n_generic.jar
  ```

  Note: The installer will fail if you attempt to run it from a network location that is specified as a UNC path. Either the JAR must be copied to the local drive, or the network path must be mapped as a network drive.

3. Welcome screen

   Click **Next**.

4. Choose Middleware Home Directory screen

   Select **Create a new Middleware Home**.

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

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

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

   If you are installing WebLogic Server 10.3.6 on both Linux and Windows machines for a mixed operating system cluster, the Middleware home (*`MW_HOME`*) and WebLogic Server home (*`WL_HOME`*) paths should match in everything but the drive letter in both the Linux and Windows installations. If the directory structures do not match exactly, the pack and unpack process will have issues when unpacking the domain on the Windows machine.

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

   - **UNIX path:** *`MW_HOME`*`/coherence_3.`*`n`*
   - **Windows path:** *`MW_HOME`*`\coherence_3.`*`n`*

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

   Click **Next**.

8. Optional screens on Windows operating system only:

   a. Choose Shortcut Location

      Specify a location for creating a shortcut to Oracle products, and click **Next**.

   b. Install Windows Service

      Specify whether or not to install **Node Manager Service**, and click **Next**.

9. Installation Summary screen

   Click **Next**.

10. Installation Progress screen

    No action is required on this screen.

11. Installation Complete screen

    Deselect **Run Quickstart**.

    Click **Done**.

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

2.4 Using the Installer for Oracle WebCenter Content

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

- Oracle WebCenter Content (WebCenter Content, which includes Oracle WebCenter Content Server)
- Oracle WebCenter Content: Inbound Refinery
- Oracle WebCenter Content: Imaging (which includes the Imaging Viewer Cache and AXF for BPEL)
- Oracle WebCenter Content: AXF for BPM
- Oracle WebCenter Enterprise Capture
- Oracle Information Rights Management (Oracle IRM)
- Oracle WebCenter Content: Records

> **Note:** If you plan to use Oracle SOA Suite with Imaging, such as for AXF for BPM or AXF for BPEL, you need to install and configure Oracle SOA Suite first. For information about installing and configuring Oracle SOA Suite, see the *Oracle Fusion Middleware Installation Guide for Oracle SOA Suite and Oracle Business Process Management Suite*.

After you install Oracle WebCenter Content and create application schemas, you can deploy any of these products to an Oracle WebLogic Server domain, as applications, by creating or extending an Oracle WebLogic Server domain, as described in Chapter 3, "Configuring Oracle WebCenter Content Applications." For information about application schemas, see Section 2.2, "Creating Oracle WebCenter Content Schemas with the Repository Creation Utility."

2.4.1 Starting the Installer

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

- **UNIX command:**

  ```
  wcc_media_loc/Disk1/runInstaller -jreLoc jre_location
  ```

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

- **Windows command:**

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

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

The installer requires the location of a Java Runtime Environment (JRE) on your system. You will need to invoke the installer with a supported JDK for your platform.

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

Notes:

- Running the installer as the user `root` is not supported.
- When you start the Oracle Fusion Middleware 11*g* WebCenter Content Installer on WebSphere Application Server, you must specify the `-jreLoc` option. For more information, see "Special Instructions When Installing Oracle Fusion Middleware with IBM WebSphere" in the *Third-Party Application Server Guide*.
- If you are using the IBM JDK with Oracle WebCenter Content and an IBM WebSphere Application Server version earlier than 7.0.0.27, certain functionality, such as the check for patches feature, will not work correctly unless the Java socket factories are changed. The IBM JRE has its own Secure Sockets Layer (SSL) socket factories. For more information, see "Changing Java Socket Factories in the IBM JDK" in the *Third-Party Application Server Guide*.

2.4.2 Following the Installation Instructions

After you have started the installer, as described in Section 2.4.1, follow the instructions in Table 2–1 to install Oracle WebCenter Content.

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

Table 2–1 Installation Procedure for Oracle WebCenter Content

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

Table 2–1 (Cont.) Installation Procedure for Oracle WebCenter Content

Screen	When This Screen Appears	Description and Action to Take
Specify Installation Location	Always	Specify the Middleware home (*MW_HOME*) and WebCenter Content Oracle home (*WCC_ORACLE_HOME*) locations. Enter values into the following fields: ■ **Oracle Middleware Home:** Select the Middleware home directory (*MW_HOME*, which was created during the installation of Oracle WebLogic Server). The default Oracle Middleware home is *user_home*/Oracle/Middleware on a UNIX operating system or *user_home*\Oracle\Middleware on a Windows operating system. ■ **Oracle Home Directory:** Specify the directory where you want to install Oracle WebCenter Content. For Oracle WebLogic Server, if you specify a directory that already exists, it must be empty and inside the Middleware home directory. If you specify a new directory, the installer creates it inside the Middleware home directory. The installation directory becomes the WebCenter Content Oracle home, represented by *WCC_ORACLE_HOME* in path names. Runtime components cannot write to this directory. The default WebCenter Content Oracle home is MW_HOME/Oracle_ECM1 on a UNIX operating system or MW_HOME\Oracle_ECM1 on a Windows operating system. If you are installing Oracle WebCenter Content on both Linux and Windows machines for a mixed operating system cluster, the Oracle home paths for Oracle WebCenter Content (*WCC_ORACLE_HOME*) should match in everything but the drive letter in both the Linux and Windows installations. If the directory structures do not match exactly, the pack and unpack process will have issues when unpacking the domain on the Windows machine. **Note:** This document refers to this directory as the WebCenter Content Oracle home to avoid confusion with the Oracle home directories of other Java components of Oracle Fusion Middleware. For more information, see "Oracle Home and Oracle Common Home Directories" in the *Installation Planning Guide*. Click **Next** to continue.
Application Server	Always	Select **WebLogic Server** to install Oracle WebCenter Content on an Oracle WebLogic Server. If you have an IBM WebSphere Application Server installed, you can select **WebSphere Server** to install Oracle WebCenter Content on an IBM WebSphere Application Server. For more information about the rest of the installation on this application server, see "Installing and Configuring Oracle Fusion Middleware on IBM WebSphere" and "Managing Oracle WebCenter Content on IBM WebSphere Application Servers" in the *Third-Party Application Server Guide*.

Table 2–1 (Cont.) Installation Procedure for Oracle WebCenter Content

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

2.5 Verifying the Installation

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

2.5.1 Viewing the Installation Log File

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

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

2.5.2 Checking the Directory Structure

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

3 Configuring Oracle WebCenter Content Applications

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

This chapter includes the following sections:

- Section 3.1, "Preparing to Configure Oracle WebCenter Content Applications"
- Section 3.2, "Creating an Oracle WebLogic Server Domain"
- Section 3.3, "Extending an Existing Domain"
- Section 3.4, "Extending a Domain in an SSL Environment"
- Section 3.5, "Increasing the Java VM Heap Size for Managed Servers"
- Section 3.6, "Setting Up Fonts on a UNIX System"
- Section 3.7, "Installing Libraries and Setting Environment Variables"
- Section 3.8, "Configuring SSL for Oracle WebCenter Content Applications"
- Section 3.9, "Reassociating the Identity Store with an External LDAP Authentication Provider"
- Section 3.10, "Adding Users to Oracle Internet Directory"
- Section 3.11, "Configuring Single Sign-On (SSO)"
- Section 3.12, "Integrating Oracle Web Tier with WebCenter Content"
- Section 3.13, "Configuring Managed Server Clusters"
- Section 3.14, "Setting Up Oracle Web Services Manager Security"

3.1 Preparing to Configure Oracle WebCenter Content Applications

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

- Oracle WebCenter Content (which includes Oracle WebCenter Content Server)
- Oracle WebCenter Content: Inbound Refinery
- Oracle WebCenter Content: Imaging (which includes the Imaging Viewer Cache and AXF for BPEL)
- Oracle WebCenter Content: AXF for BPM

- Oracle WebCenter Enterprise Capture
- Oracle Information Rights Management
- Oracle WebCenter Content: Records

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

Notes:

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

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

Notes:

- WebCenter Content cannot be deployed to the same domain as Oracle Identity Manager and Oracle Identity Management.
- Oracle WebCenter Content 11*g* does not support running WebCenter Content, Inbound Refinery, Records, or Oracle IRM as a service on a Windows operating system.

For Imaging to take advantage of Business Process Management (BPM) and Oracle BPEL Process Manager within an existing domain, the domain must be extended with Oracle BPM Suite. If you want to use Oracle BPEL Process Manager and not BPM, you can extend the domain with Oracle SOA Suite. For information about connecting to

BPM or Oracle BPEL Process Manager as a workflow server, see Section 6.1.4, "Connecting to a Workflow Server."

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

If you have not successfully run the installer on your system, first see Chapter 2, "Installing Oracle WebCenter Content."

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

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

> **Note:** You cannot extend a domain that has an Oracle Enterprise Content Management Suite or Oracle WebCenter Content application from an earlier release to include an Oracle WebCenter Content 11.1.1.9.0 application.

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

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

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

3.2 Creating an Oracle WebLogic Server Domain

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

> **Note:** If you plan to use Oracle SOA Suite with Imaging, such as for AXF for BPM or AXF for BPEL, you need to install and configure Oracle SOA Suite first. For information about installing and configuring Oracle SOA Suite, see the *Oracle Fusion Middleware Installation Guide for Oracle SOA Suite and Oracle Business Process Management Suite*.
>
> If you create the domain with Oracle SOA Suite, you can extend the domain with Oracle WebCenter Content, as described in Section 3.3, "Extending an Existing Domain."

The configuration wizard is in the following directory. *WCC_ORACLE_HOME* represents the WebCenter Content Oracle home directory, where Oracle WebCenter Content is installed. The WebCenter Content Oracle home was specified in the **Oracle Home Directory** field on the Specify Installation Location screen of the installer (default `Oracle_ECM1`).

- **UNIX path:** *WCC_ORACLE_HOME*`/common/bin`
- **Windows path:** *WCC_ORACLE_HOME*`\common\bin`

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

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

  Your log file will be created in the location from which you start the configuration wizard.

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

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

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

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

Table 3–1 Procedure for Creating a New Domain

Screen	When This Screen Appears	Description and Action to Take
None		Start Fusion Middleware Configuration Wizard: ■ **UNIX script:** *WCC_ORACLE_HOME*/common/bin/config.sh[-log=*log_file_name*] ■ **Windows script:** *WCC_ORACLE_HOME*\common\bin\config.cmd[-log=*log_file_name*]
Welcome	Always	Select **Create a new WebLogic Domain**. Click **Next** to continue.
Select Domain Source	Always	Select **Generate a domain configured automatically to support the following products**, and then select one or more of these product templates: ■ **Oracle WebCenter Content: AXF for BPM** ■ **Oracle WebCenter Enterprise Capture** ■ **Oracle WebCenter Content: Imaging** ■ **Oracle Universal Records Management** (for Oracle WebCenter Content: Records) ■ **Oracle Universal Content Management - Inbound Refinery** (for Oracle WebCenter Content: Inbound Refinery) ■ **Oracle Universal Content Management - Content Server** (for Oracle WebCenter Content) ■ **Oracle Information Rights Management**
		For WebCenter Content: Select **Oracle Universal Content Management - Content Server**.
		For Imaging: When you select **Oracle WebCenter Content: Imaging**, you also need to select **Oracle Universal Content Management - Content Server**.
		For Imaging Viewer Cache When you select **Oracle WebCenter Content: Imaging, Oracle WebCenter Content: Imaging Viewer Cache** is automatically selected.
		For AXF for BPEL: Imaging includes AXF for BPEL. Select **Oracle WebCenter Content: Imaging** and **Oracle Universal Content Management - Content Server**.

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

Screen	When This Screen Appears	Description and Action to Take
		For AXF for BPM: If you are going to use AXF for BPM with Imaging, you need to select the following product templates (some of these are automatically selected): ■ **Oracle BPM Suite** ■ **Oracle SOA Suite** ■ **Oracle WebCenter Content: AXF for BPM** ■ **Oracle WebCenter Content: Imaging Viewer Cache** ■ **Oracle WebCenter Content: Imaging** ■ **Oracle Universal Content Management - Content Server** ■ **Oracle Enterprise Manager** ■ **Oracle WSM Policy Manager** ■ **Oracle JRF**
		For AXF for BPM or AXF for BPEL with Oracle SOA Suite on a different domain or machine: If you are going to use AXF for BPM or AXF for BPEL with Imaging, and Oracle SOA Suite is deployed to a different domain or installed on a different machine, you will need to run `WCC_ORACLE_HOME\common\config.cmd` on the Oracle SOA Suite machine and select the following product templates: ■ **Oracle SOA Suite** ■ **Oracle WSM Policy Manager** ■ **Oracle Enterprise Manager**
		For Oracle WebCenter Enterprise Capture: Select the following product templates (some of these are automatically selected): ■ **Oracle WebCenter Enterprise Capture** ■ **Oracle Enterprise Manager** ■ **Oracle JRF**
		For Site Studio for External Applications: If you want a remote deployment of a Site Studio for External Applications website, you can select **Oracle Universal Content Management - SSXA Server** (for Oracle WebCenter Content - SSXA Server) to create an Oracle WebLogic Server domain with a Managed Server that has the files required to run the website.
		For Oracle WSM Policy Manager: To create a domain that includes Oracle Web Services Manager (Oracle WSM) Policy Manager, select **Oracle WSM Policy Manager**.
		For Oracle Enterprise Manager and Oracle JRF When you select any Oracle WebCenter Content application on the Select Domain Source screen, **Oracle Enterprise Manager** and **Oracle JRF** are automatically selected. If you deselect any of these items that are automatically selected, the Oracle WebCenter Content application will also be deselected.

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

Screen	When This Screen Appears	Description and Action to Take
		Click **Next** to continue.
Specify Domain Name and Location	Always	Enter the name of the domain you want to create in the **Domain name** field. The default location for the domain follows (*`MW_HOME`* represents the Middleware home directory): ■ **UNIX path:** *`MW_HOME`*`/user_projects/domains` ■ **Windows path:** *`MW_HOME`*`\user_projects\domains` You can specify a different location in the **Domain location** field. **Note:** Record the domain name and location from this screen because you will need them later to start the Administration Server. You can specify the location of the Oracle WebCenter Content application in the **Application location** field. The default location is *`MW_HOME`*`/user_projects/applications/`. Click **Next** to continue.
Configure Administrator User Name and Password	Always	The **Name** field has the default administrator user name, `weblogic`. You can specify a different administrator user name. In the **User password** field, enter the password for the administrator user. Then enter it again in the **Confirm user password** field. **Note:** Record the administrator user name and password from this screen because you will need them later to start the Managed Servers and to access the domain through the Oracle WebLogic Server Administration Console or Fusion Middleware Control. Click **Next** to continue.
Configure Server Start Mode and JDK	Always	Under WebLogic Domain Startup Mode, **Development Mode** is the default mode. For a production system, select **Production Mode**. Under JDK Selection, you can leave **Available JDKs** and the default JDK selected, or you can change them. The default JDK for development mode is **Sun SDK** ***version***, and the default JDK for production mode is **JRockit SDK** ***version***, except on a 64-bit system, where the default JDK is the one you installed. To specify a different JDK, select **Other JDK**, and enter its location. Click **Next** to continue.

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

Screen	When This Screen Appears	Description and Action to Take
Configure JDBC Component Schema	Always	Configure each component schema, including the Oracle WSM MDS schema if it was created with Repository Creation Utility (RCU), by selecting a schema checkbox and then completing the following fields: ■ **Component Schema:** Select a component schema row. ■ **Vendor:** Select a database vendor from the list. ■ **Driver:** Leave the default driver for the database vendor selected, or select a driver for the component schema from the list. ■ **Schema Owner:** Enter the user name of the application schema owner, specified during schema creation with RCU. ■ **Schema Password:** Enter the schema password, specified during schema creation with RCU. ■ **DBMS/Service:** Enter the name of the database instance if `Oracle's Driver (Thin) for Instance connections` is selected in the **Driver** field, or enter the service name (global database name) if `Oracle's Driver (Thin) for Service connections` is selected in the **Driver** field. For Microsoft SQL Server or IBM DB2, you must enter a database name because there is no service name. Specify the database that contains the application schema or schemas. For IBM DB2, if the name of the schema suffix displayed on the screen is longer than 3 characters, you need to change it to the name specified for the schema when it was created in the Repository Creation Utility (see Section 2.2.2, "Creating Schemas for Oracle WebCenter Content Applications"). For example, change `DEV_CAPTURE` to `DEV_ODC`, `DEV_URMSERVER` to `DEV_URM`, or `DEV_ORAIRM` to `DEV_IRM`. For Oracle RAC databases, specify the service name of one of the nodes in this field. For example: `sales.example.com`. ■ **Host Name:** Specify the name of the machine on which your database resides, in the format `host.example.com`. For Oracle RAC databases, specify the Virtual IP name or one of the node names as the host name. ■ **Listen Port:** Specify the database listen port number. The default port number is 1521 for an Oracle Database instance, `1433` for Microsoft SQL Server, or `50000` for IBM DB2. Click **Next** to continue.
Test Component Schema	Always	The configuration wizard automatically tests the connection to the JDBC component schema. If the test fails, click **Previous** to correct the component schema information, and then click **Next** to retest the connection. After the test succeeds, click **Next** to continue.

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

Screen	When This Screen Appears	Description and Action to Take
Select Optional Configuration	Always	Optionally, select any or all of these options for configuring the Administration Server and Managed Servers: - **Administration Server** - **JMS Distributed Destination** - **Managed Servers, Clusters and Machines** - **Deployments and Services** - **RDBMS Security Store** Select one or more of these options if you want to change any default settings. For example, select **Administration Server** to configure SSL for it or change its port number, or select **Managed Servers, Clusters and Machines** to change the name or port for a Managed Server, add it to a cluster, or configure a machine for it. If you are configuring an Oracle WebCenter Enterprise Capture cluster with Managed Servers in both Linux and Windows environments, select all except the last option. For Oracle IRM, you should select **Administration Server**, **Managed Servers, Clusters and Machines**, and **Deployments and Services**. **Note:** To use clusters, you need a license for Oracle WebLogic Server Enterprise Edition. Click **Next** to continue to the configuration screens for the selected option or, if you did not select any options, to the Configuration Summary screen.
Configure the Administration Server	If you selected **Administration Server** on the Select Optional Configuration screen	The default listen port number for the Administration Server is `7001`, which you can change. If you want to change the configuration of SSL for the Administration Server, you can select **SSL enabled**. The SSL port is set to 7002 by default in the **SSL Listen Port** field. If **SSL enabled** is selected, you can change the SSL listen port value. For more information about SSL configuration, see Section 3.8, "Configuring SSL for Oracle WebCenter Content Applications." Click **Next** to continue.
Select JMS Distributed Destination Type	If you selected **Oracle WebCenter Content: Imaging** on the Select Domain Source screen	Accept the default (UDD), and click **Next**. Click **OK** in the override warning.

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

Screen	When This Screen Appears	Description and Action to Take

Configure Managed Servers	If you selected **Managed Servers, Clusters and Machines** on the Select Optional Configuration screen	Each Managed Server needs a unique listen port number. For each Managed Server, you can use the default **Listen port** value. For increased security, you can specify a nondefault port number.
		Table 3–2 lists the default port values for the Managed Servers that run Oracle WebCenter Content applications.
		If you want to change the SSL configuration for a Managed Server, you can select **SSL enabled** and set or change the **SSL listen port** value.
		For a mixed Oracle WebCenter Enterprise Capture cluster, configure two Managed Servers, one for a Linux environment and one for a Windows environment, with different **Listen address** values and the same **Listen port** value. For example:
		`Name` **`Listen address`** **`Listen port`**
		`capture_lnx_server1` *`host-ip-address`* `16400`
		`capture_win_server2` *`host-ip-address`* `16400`
		For Oracle IRM, SSL is enabled by default, with port number `16101`. SSL needs to be configured so that Content application server Desktop does not show prompts to accept certificates when it contacts the Managed Server. The certificate used must be trusted by Microsoft Internet Explorer on computers running Oracle IRM Desktop.
		Click **Next** to continue.

Configure Clusters	If you selected **Managed Servers, Clusters and Machines** on the Select Optional Configuration screen.	Optionally, configure one or more clusters. For example, for an Oracle WebCenter Enterprise Capture cluster of two Managed Servers, one in a linux environment and the other in a Windows environment, create a cluster named `cap_cluster` with the **Cluster messaging mode** value `unicast`. **Notes:** ■ To use clusters, you need a license for Oracle WebLogic Server Enterprise Edition. ■ If you decide to configure a cluster, then you must assign a cluster address. Click **Next** to continue.
Assign Servers to Clusters	If you configured any clusters on the Configure Clusters screen	Assign two or more of the Managed Servers in the domain to each cluster. For example, for a mixed Oracle WebCenter Enterprise Capture cluster, assign the Managed Servers `capture_lnx_server1` (configured to run in a Linux environment) and `capture_win_server2` (configured to run in a Windows environment) to cap_cluster. Click **Next** to continue.
Create HTTP Proxy Applications	If you configured any clusters on the Configure Clusters screen and assigned some, but not all, of the Managed Servers in the domain to a cluster	Create a proxy application for each Managed Server that you did not assign to a cluster in the domain. Click **Next** to continue.

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

Screen	When This Screen Appears	Description and Action to Take
Configure Machines	If you selected **Managed Servers, Clusters and Machines** on the Select Optional Configuration screen	Optionally, configure machines to host Managed Servers, and assign a Managed Server to each machine. Click **Next** to continue.
Assign Servers to Machines	If you added any machines on the Configure Machines screen	Assign at least one server to each machine. Click **Next** to continue.
Target Deployments to Clusters or Servers	If you selected **Deployments and Services** on the Select Optional Configuration screen	Optionally, assign each application to the Administration Server, a Managed Server, or a cluster of Managed Servers. Oracle IRM should be deployed on a cluster or on a Managed Server that is not a member of any cluster because Oracle IRM uses `persistent-store-type` as `replicated_if_clustered`. If the Oracle IRM web application is deployed on a clustered server, the in-effect `persistent-store-type` value will be replicated. Otherwise, `memory` is the default. When deploying Oracle IRM to a cluster, make sure that the Oracle IRM application is deployed to all nodes. Click **Next** to continue.
Target Services to Clusters or Servers	If you selected **Deployments and Services** on the Select Optional Configuration screen	Optionally, modify how your services are targeted to servers or clusters. Click **Next** to continue.
Configure RDBMS Security Store Database	If you selected **RDBMS Security Store** on the Select Optional Configuration screen	Optionally, make changes to your RDBMS security store. Click **Next** to continue.
Configuration Summary	Always	Review your configuration and make any corrections or updates by following the instructions on the screen. You can click **Previous** on each screen to go back to a screen where you want to change the configuration. When the configuration is satisfactory, click **Create** to create the domain.
Creating Domain	Always	On a Windows operating system, you can select **Start Admin Server** to start the Administration Server as soon as the configuration is done. When the domain is created successfully, click **Done**.

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

Table 3–2 Default Ports for Managed Servers

Managed Server	Default Listen Port	Default SSL Port	Port Range
Imaging	`16000`	`16001`	`16000-16099`
Oracle IRM	`16100`	`16101`	`16100-16199`
WebCenter Content	`16200`	`16201`	`16200-16299`

Table 3–2 (Cont.) Default Ports for Managed Servers

Managed Server	Default Listen Port	Default SSL Port	Port Range
Inbound Refinery	`16250`	`16251`	`16200-16299`
Records	`16300`	`16301`	`16300-16399`
Oracle WebCenter Enterprise Capture	`16400`	`16401`	`16400-16499`

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."

3.3 Extending an Existing Domain

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

- **UNIX path:** `WCC_ORACLE_HOME/common/bin`
- **Windows path:** `WCC_ORACLE_HOME\common\bin`

Notes:

- WebCenter Content cannot be deployed to the same domain as Oracle Identity Manager and Oracle Identity Management.
- You cannot extend a domain that has an Oracle Enterprise Content Management Suite or Oracle WebCenter Content application from an earlier release to include an Oracle WebCenter Content 11.1.1.9.0 application.

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

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

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

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

Table 3–3 Procedure for Extending an Existing Domain

Screen	When This Screen Appears	Description and Action to Take
None.	Always	Start Fusion Middleware Configuration Wizard: - **UNIX script:** `WCC_ORACLE_HOME/common/bin/config.sh [-log=log_file_name]` - **Windows script:** `WCC_ORACLE_HOME\common\bin\config.cmd [-log=log_file_name]`
Welcome	Always	Select **Extend an existing WebLogic Domain**. Click **Next** to continue.
Select a WebLogic Domain Directory	Always	Select a directory for adding your applications or services, or both. Click **Next** to continue.
Select Extension Source	Always	Select **Extend my domain automatically to support the following added products**, and then select one or more of these product templates: - **Oracle WebCenter Content: AXF for BPM** - **Oracle WebCenter Content: Imaging** - **Oracle WebCenter Enterprise Capture** - **Oracle Universal Records Management** (for Oracle WebCenter Content: Records) - **Oracle Universal Content Management - Inbound Refinery** (for Oracle WebCenter Content: Inbound Refinery) - **Oracle Universal Content Management - Content Server** (for Oracle WebCenter Content) - **Oracle Information Rights Management**
		For WebCenter Content: Select **Oracle Universal Content Management - Content Server**.
		For Imaging: When you select **Oracle WebCenter Content: Imaging**, you also need to select **Oracle Universal Content Management - Content Server** if WebCenter Content is not already configured in the domain.
		For Imaging Viewer Cache When you select **Oracle WebCenter Content: Imaging, Oracle WebCenter Content: Imaging Viewer Cache** is automatically selected.
		For AXF for BPEL: Imaging includes AXF for BPEL. Select **Oracle WebCenter Content: Imaging** and **Oracle Universal Content Management - Content Server**.

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

Screen	When This Screen Appears	Description and Action to Take
		For AXF for BPM: If you are going to use AXF for BPM with Imaging, you need to select the following product templates (some of these are automatically selected): ■ **Oracle BPM Suite** ■ **Oracle SOA Suite** ■ **Oracle WebCenter Content: AXF for BPM** ■ **Oracle WebCenter Content: Imaging Viewer Cache** ■ **Oracle WebCenter Content: Imaging** ■ **Oracle Universal Content Management - Content Server** ■ **Oracle Enterprise Manager** ■ **Oracle WSM Policy Manager** ■ **Oracle JRF**
		For AXF for BPM or AXF for BPEL with Oracle SOA Suite on a different domain or machine: If you are going to use AXF for BPM or AXF for BPEL with Imaging, and Oracle SOA Suite is deployed to a different domain or installed on a different machine, you will need to run `*WCC_ORACLE_HOME*\common\config.cmd` on the Oracle SOA Suite machine and select the following product templates: ■ **Oracle SOA Suite** ■ **Oracle WSM Policy Manager** ■ **Oracle Enterprise Manager**
		For Oracle WebCenter Enterprise Capture: Select the following product templates (some of these are automatically selected): ■ **Oracle WebCenter Enterprise Capture** ■ **Oracle Enterprise Manager** ■ **Oracle JRF**
		For Site Studio for External Applications: If you want a remote deployment of a Site Studio for External Applications website, you can select **Oracle Universal Content Management - SSXA Server** (for Oracle WebCenter Content - SSXA Server) to extend an Oracle WebLogic Server domain with a Managed Server that has the files required to run the website.
		For Oracle WSM Policy Manager: To extend a domain with Oracle Web Services Manager (Oracle WSM) Policy Manager, select **Oracle WSM Policy Manager**.
		Oracle Enterprise Manager and Oracle JRF When you select any Oracle WebCenter Content application, **Oracle Enterprise Manager** and **Oracle JRF** are automatically selected. If you deselect any of these items that are automatically selected, the Oracle WebCenter Content application will also be deselected.

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

Screen	When This Screen Appears	Description and Action to Take
		Click **Next** to continue.
Configure JDBC Component Schema	Always	Configure each component schema, including the Oracle WSM MDS schema if it was created with Repository Creation Utility (RCU), in the following fields: ■ **Component Schema:** Select a component schema row. ■ **Vendor:** Select a database vendor from the list. ■ **Driver:** Leave the default driver for the database vendor selected, or select a driver for the component schema from the list. ■ **Schema Owner:** Enter the user name of the application schema owner, specified during schema creation with RCU. ■ **Schema Password:** Enter the schema password, specified during schema creation with RCU.
		■ **DBMS/Service:** Enter the name of the database instance if `Oracle's Driver (Thin) for Instance connections` is selected in the **Driver** field, or enter the service name (global database name) if `Oracle's Driver (Thin) for Service connections` is selected in the **Driver** field. For Microsoft SQL Server, you must enter a database name because there is no service name. Specify the database that contains the application schema or schemas. For IBM DB2, if the name of the schema suffix displayed on the screen is longer than 3 characters, you need to change it to the name specified for the schema when it was created in the Repository Creation Utility (see Section 2.2.2, "Creating Schemas for Oracle WebCenter Content Applications"). For example, change `DEV_CAPTURE` to `DEV_ODC`, `DEV_URMSERVER` to `DEV_URM`, and `DEV_ORAIRM` to `DEV_IRM`. For Oracle RAC databases, specify the service name of one of the nodes in this field. For example: `sales.example.com`. ■ **Host Name:** Specify the name of the machine on which your database resides, in the format `host.example.com`. For Oracle RAC databases, specify the Virtual IP name or one of the node names as the host name. ■ **Listen Port:** Specify the database listen port number. The default port number is 1521 for an Oracle Database instance, `1433` for Microsoft SQL Server, or `50000` for IBM DB2. Click **Next** to continue.
Test Component Schema	Always	The configuration wizard automatically tests the connection to the JDBC component schema. If the test fails, click **Previous** to correct the component schema information, and then click **Next** to retest the connection. After the test succeeds, click **Next** to continue.

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

Screen	When This Screen Appears	Description and Action to Take
Select Optional Configuration	Always	Optionally, select any or all of these options for configuring Managed Servers: - **JMS Distributed Destination** - **Managed Servers, Clusters and Machines** - **Deployments and Services** - **RDBMS Security Store** Select one or more of these options if you want to change any default settings. For example, select **Administration Server** to configure SSL for it or change its port number, or select **Managed Servers, Clusters and Machines** to change the name or port for a Managed Server, add it to a cluster, or configure a machine for it. **Note:** To use clusters, you need a license for Oracle WebLogic Server Enterprise Edition. For Oracle IRM, you should select **Administration Server**, **Managed Servers, Clusters and Machines**, and **Deployments and Services**. If you are extending a domain that already includes WebCenter Content with Imaging and plan to use WebCenter Content 11*g* as the Imaging repository, select **Managed Servers, Clusters and Machines** so you can configure a separate machine for running the Imaging Managed Server. Click **Next** to continue to the configuration screens for the selected option, or if you did not select any options, to the Configuration Summary screen.
Select JMS Distributed Destination Type	If you selected **Oracle WebCenter Content: Imaging** on the Select Extension Source screen	Accept the default (UDD), and click **Next**. Click **OK** in the override warning.
Configure Managed Servers	If you selected **Managed Servers, Clusters and Machines** on the Select Optional Configuration screen	Each Managed Server needs a unique listen port number. For each Managed Server, you can use the default **Listen port** value or, for increased security, specify a nondefault port number. Table 3–2 lists the default port values for the Managed Servers that run Oracle WebCenter Content applications. To change the SSL configuration for a Managed Server, you can select **SSL enabled** and set or change the **SSL listen port** value. For Oracle IRM, SSL is enabled by default, with port number `16101`. SSL needs to be configured so that Oracle IRM Desktop does not show prompts to accept certificates when it contacts the Managed Server. The certificate used must be trusted by Microsoft Internet Explorer on computers running Oracle IRM Desktop. Click **Next** to continue.

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

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

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

Screen	When This Screen Appears	Description and Action to Take
Target Services to Clusters or Servers	If you selected **Deployments and Services** on the Select Optional Configuration	Optionally, modify how your services are targeted to servers or clusters. Click **Next** to continue.
Configuration Summary	Always.	When the configuration is satisfactory, click **Extend** to extend the domain.
Extending 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."

3.4 Extending a Domain in an SSL Environment

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

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

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

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

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

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

- URL:

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

- Properties:

  – `user=MAR20SSL_OCS`

  – `oracle.net.CONNECT_TIMEOUT=10000`

  – `sendStreamAsBlob=true`

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

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

   - URL:

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

   - Properties:

     – `javax.net.ssl.trustStorePassword=`*`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.

3.5 Increasing the Java VM Heap Size for Managed Servers

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

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

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

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

  This method is required if the Managed Server process will be run from Node Manager. For more information about running Managed Servers from Node Manager, see Section 10.4, "Using Node Manager with Oracle WebCenter Content."

- Setting the USER_MEM_ARGS Environment Variable for a Managed Server

  This method is required if the Managed Server process will be run directly from the command line. For more information about running Managed Servers from the command line, see Section 10.2, "Starting Managed Servers."

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

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

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

1. Start the Administration Server for your Oracle WebLogic Server domain, as described in Section 10.1, "Starting the Administration Server."
2. 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.
3. Click **Environment** under Domain Structure, on the left.
4. Click **Servers** on the Summary of Environment page.
5. Set the memory parameters for each Managed Server:

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

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

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

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

Table 3–4 Java VM Memory Parameters

Java VM	Operating System	Parameters
Sun JDK	UNIX	`-Xms256m -Xmx1024m -XX:CompileThreshold=8000 -XX:PermSize=128m -XX:MaxPermSize=512m`
Sun JDK	Windows	`-Xms256m -Xmx1024m -XX:CompileThreshold=8000 -XX:PermSize=128m -XX:MaxPermSize=512m`[1]
Oracle JRockit	UNIX	`-Xms256m -Xmx1024m -XnoOpt`
Oracle JRockit	Windows	`-Xms256m -Xmx1024m -XnoOpt`

[1] See information in preceding text about the heap size on a Windows system.

d. Save the configuration changes.

6. Restart any running Managed Servers, as described in Section 10.3, "Restarting a Managed Server."

3.5.2 Setting the USER_MEM_ARGS Environment Variable for a Managed Server

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

To set the USER_MEM_ARGS Environment Variable for a Managed Server:

- UNIX shell script (`.sh`) entry

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

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

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

- Windows command file (`.cmd`) entry

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

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

3.6 Setting Up Fonts on a UNIX System

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

3.6.1 Setting Up TrueType Fonts on a UNIX System

For Imaging and WebCenter Content Dynamic Converter to work best on a UNIX operating system, you can set up TrueType fonts on the machine where Imaging, Inbound Refinery, or the Dynamic Converter is running. If these fonts are not available on your system, you need to install them. Inbound Refinery and Content Server default to the TrueType fonts in the JRE, at `JAVA_HOME/lib/fonts`. For information about configuring the path to the font directory for Imaging once the fonts are installed, see Section 6.1.5, "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`
- Solaris X64: `/usr/openwin/lib/X11/fonts/TrueType`
- AIX: `/usr/lpp/X11/lib/X11/fonts/TrueType`
- HP-UX Itanium: `/usr/lib/X11/fonts/TrueType`
- HP-UX PARISC64: `/usr/lib/X11/fonts/TrueType`
- Linux: `/usr/lib/X11/fonts/TrueType`

To set the path to the font directory in Inbound Refinery:

1. Log in to Inbound Refinery.
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**.

3.6.2 Installing Fonts for National Language Support on a UNIX System

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

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

3.7 Installing Libraries and Setting Environment Variables

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

Note: The Outside In Technology binaries are 32 bit, so your system needs to be capable of running 32-bit binaries and have compatible libraries installed.

3.7.1 Installing Libraries on UNIX Platforms

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

Many of the required libraries are normally installed on the machine, including the C, math, X11, dynamic loader, and pthreads libraries, among others.

- Solaris SPARC 32-bit or 64-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
libgen.so.1
libm.so.1
libmp.so.2
libnsl.so.1
libpthread.so.1
libsocket.so.1
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
libm.so.1
libpthread.so.1
libstd_v2.so.1
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.

- Linux variants

  For Linux variants, the file `/lib/libz.so.1` is required.

3.7.2 Setting Library Paths in Environment Variables on UNIX Platforms

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

- Environment variables for library paths for Imaging
  - Add the following line to the Inbound Refinery `intradoc.cfg` file at *`DomainHome`*`/ucm/ibr/bin`:

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

    Then restart Inbound Refinery, as described in Section 10.3, "Restarting a Managed Server."
  - AIX:

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

  - HP-UX Itanium:

    ```
    LD_LIBRARY_PATH=DomainHome/oracle/imaging/imaging-server:"$LD_LIBRARY_PATH"
    ```

- DISPLAY environment variable

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

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

For correct operation of WebCenter Content, Inbound Refinery, or Records on a Windows operating system, you need to have the Visual C++ libraries that are included in the Visual C++ Redistributable Package. Different versions of this package are available from the Microsoft Download Center at

`http://www.microsoft.com/downloads`

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

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

The required versions of each of these downloads are the Microsoft Visual C++ 2005 SP1 Redistributable Package and Microsoft Visual C++ 2008 SP1 Redistributable Package. The required redistributable module is `msvcr80.dll`.

Notes:

- Before you can commit a document using the PDF Searchable Document Output Format on a Windows system, the Microsoft Visual C++ 2010 Redistributable Package must be installed. If this package is not already on your system, you can download it from Microsoft. Microsoft .NET Framework 4.0 is also required, which if not already present, needs to be installed.
- For a list of platforms that support the PDF Searchable Document Output Format, see the "Oracle WebCenter Content 11g Release 1 (11.1.1.x) Certification Matrix," available in the "System Requirements and Supported Platforms for Oracle WebCenter Content 11gR1" document on the Oracle Fusion Middleware Supported System Configurations page at

  http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html

Inbound Refinery configuration on a Windows x64 operating system requires Visual Studio 2005 runtime support, which is `vcredist_x64.exe` for KB973544. Also, when Inbound Refinery is installed on a Windows x64 operating system, both the 32-bit and 64-bit C++ libraries are required. Content Server also requires the 32-bit libraries because it uses 32-bit Outside In Technology.

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

3.8 Configuring SSL for Oracle WebCenter Content Applications

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

Note: If SSL is enabled, before you use WLST to connect to the Administration Server, you must either append the following parameters to the `JVM_ARGS` section of the `wlst.sh` file or set them in the `CONFIG_JVM_ARGS` environment variable:

```
-Dweblogic.security.SSL.ignoreHostnameVerification=true
-Dweblogic.security.TrustKeyStore=KeyStoreName
```

`KeyStoreName` is the name of the keystore in use (`DemoTrust` for the built-in demonstration certificate). The `wlst.sh` file is in the `bin` subdirectory of the `common` directory in the WebCenter Content Oracle home directory.

3.8.1 Configuring SSL for a Production Environment

Oracle IRM requires SSL to be enabled on the front-end application, whether it is Oracle HTTP Server (OHS) or a Managed Server running Oracle IRM as an application deployed to Oracle WebLogic Server. Communication between 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 the *Administrator's Guide*.

3.8.2 Configuring SSL for a Development Environment

For a development environment, you can also configure one-way SSL with a server-specific certificate. One-way SSL means that only the server certificate passes from the server to the client but not the other way around. After you configure one-way SSL for a development environment on the server, you have to configure every client to accept the server certificate.

3.8.2.1 Configuring One-Way SSL for a Development Environment

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

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

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

To configure one-way SSL for a development environment:

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

   - **UNIX script:**
     MW_HOME/wlserver_10.3/server/bin/setWLSEnv.sh
   - **Windows script:**
     MW_HOME\wlserver_10.3\server\bin\setWLSEnv.cmd

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

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

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

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

   For `mykeypass`, substitute a password for the key, and for *`hostname`*, substitute the name of the machine that hosts the Managed Server to which the application is deployed. You should use the same name while accessing Oracle Web Services.

For example, to generate the server certificate for a machine named `myhost.us.example.com`, the command would be as follows (in a single command line):

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

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

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

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

3. Run the `ImportPrivateKey` utility to package the Private Key and Self-Signed Root Certificate into a keystore, 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 keystore named Trust Keystore.

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

   - **UNIX operating system**

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

   - **Windows operating system**

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

5. Click **Next**

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

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

   a. 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, 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. Select **Environment** under your domain from Domain Structure.

   d. Select **Servers** from **Environment**.

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

   f. Click the **Keystores** tab on the Settings for *servername* page.

   g. 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.

   h. 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

   i. Save the changes.

   j. Click the **SSL** tab.

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

   l. Enter values in the other fields on the **SSL** tab:

      Private key alias

      Private key passphrase

      Confirm Private key passphrase

   m. Save the changes.

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

3.8.2.2 Configuring Clients to Accept the Server Certificate

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

To configure clients to accept the server certificate:

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

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

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

2. In the Certificate Import Wizard, explicitly select a certificate store for **Trusted Root Certification Authorities**. The root certificate must be trusted on *all* client computers that will access the server.

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

3.9 Reassociating the Identity Store with an External LDAP Authentication Provider

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

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

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

For a production installation, Oracle Internet Directory (OID) or Oracle Database 11*g* is required for using Oracle WebCenter Enterprise Capture because Capture uses Oracle Platform Security Services (OPSS), which works only with Oracle Database for its schema.

For an AXF for BPM application, before you can access the AXF Solution Administration page, you need to set up an `axfadmin` group in the external LDAP authentication provider and assign the AXF users you want to the group.

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

1. Back up existing data with the `setIRMExportFolder` script.
2. Reassociate the identity store with an external LDAP directory.
3. Verify that all users and groups exist in target LDAP identity store.
4. Migrate data with the `setIRMImportFolder` script.

3.9.1 Reassociating the Identity Store with Oracle Internet Directory

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

You can use a similar procedure to reassociate the identity store with other LDAP authentication providers. Each provider has a specific authenticator type, and only that type should be configured. Table 3–5 lists the available authenticator types.

Table 3–5 LDAP Authenticator Types

LDAP Authentication Provider	Authenticator Type
Microsoft AD	ActiveDirectoryAuthenticator
SunOne LDAP	IPlanetAuthenticator
Directory Server Enterprise Edition (DSEE)	IPlanetAuthenticator
Oracle Internet Directory	OracleInternetDirectoryAuthenticator
Oracle Virtual Directory	OracleVirtualDirectoryAuthenticator
Oracle Unified Directory	IPlanetAuthenticator
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 the embedded LDAP provider 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 administrator 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, which uses the export folder path to decide where to write out the user and group details. The Oracle IRM Managed Server must have write access to the folder path. The export folder must exist before you run the `setIRMExportFolder` command.

   The following example sets */user/irm-data* as the export folder:

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

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

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

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

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

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

After this process is complete, reset the export folder:

```
setIRMExportFolder('')
```

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

5. Configure the Oracle Internet Directory authentication provider:

   a. Start the Administration Server for your Oracle WebLogic Server domain, as described in Section 10.1, "Starting the Administration Server."

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

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

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

   ```
   http://myHost.example.com:7001/console
   ```

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

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

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

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

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

   For a list of authenticator types for different LDAP Authentication Providers, see Table 3–5.

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

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

   i. Click **Providers** in the breadcrumb trail along the top of the page to navigate back to the **Providers** tab.

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

   The **Configuration** tab has two tabs, **Common** and **Provider Specific**. On the **Common** tab, change the **Control Flag** value to `SUFFICIENT`, and then click **Save**.

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

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

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

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

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

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

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

   ```
   cn=orcladmin
   ```

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

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

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

   ```
   cn=users,dc=example,dc=com
   ```

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

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

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

   Select this attribute for Oracle IRM.

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

   ```
   cn=groups,dc=example,dc=com
   ```

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

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

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

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

l. Click **Save**.

6. Restart the Administration Server, as described in Section 10.3, "Restarting a Managed Server."

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 **Users and Groups** tab to see a list of users contained in the configured authentication providers, on the **Users** subtab, and then click the **Groups** subtab 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.
    - If your Managed Servers are already running and configured, 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. 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 */user/irm-data* as the import folder:

```
cd WCC_ORACLE_HOME/common/bin
./wlst.sh
> connect('weblogic', 'password', 't3://adminServerHost:adminServerPort')
> setIRMImportFolder('/user/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:

```
/user
   /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`:

```
/user
   /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('/user/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 an LDAP identity store is reassociated, 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 rights 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.

3.9.2 Refreshing GUID Values in Imaging Security Tables

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

Only users and groups that exist in both LDAP providers will have GUIDs refreshed. Imaging permissions assigned to users and groups from the previous LDAP will be refreshed to the users and groups that match in the new LDAP. If users and/or groups do not match any users and/or groups in the new LDAP provider, `refreshIPMSecurity` will ignore them.

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

3.9.2.1 Refreshing GUID values in Imaging Security Tables with WLST

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

To refresh GUID values in Imaging security tables with WLST:

1. Start the Administration Server for your Oracle WebLogic Server domain, as described in Section 10.1, "Starting the Administration Server."
2. Log in to the Oracle WebLogic Server Administration Server.
3. Navigate to the Oracle WebCenter Content home directory: *`MW_HOME/WCC_ORACLE_HOME`*.
4. Invoke WLST:

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

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

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

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

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

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

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

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

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

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

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

1. Log in to Fusion Middleware Control.
2. In the navigation tree on the left, expand **WebLogic Domain**, then the Oracle WebCenter Content domain folder, then **IPM_Cluster**, and then the name of the Imaging server, such as **IPM_server1**.
3. On the right, click the **WebLogic Server** drop-down menu, and choose **System MBean Browser**.
4. In the System MBean Browser navigation tree, expand **Application Defined MBeans**, then **oracle.imaging**, then **Server: IPM_server1**, and then **cmd**, and click **cmd**.
5. Click **refreshIPMSecurity** on the right.
6. Press the **Invoke** button.
7. Log in to Imaging to verify user and group security.

3.9.3 Configuring an LDAP Authentication Provider for Performance

When configuring an LDAP authentication provider, you can avoid significant performance issues by configuring the DNs at the highest level possible. This is true for both the `User Base DN` and `Group Base DN` configuration options.

The `Group Base DN` value is especially important because getting the groups associated with users can cause many queries to be executed against the LDAP server. This can cause significant performance issues depending on the number of directly assigned groups as well as the groups assigned indirectly as subgroups of other groups. You can easily default these settings to the root DN, but the root DN is not optimal because using a top-level DN provides access to all the groups under the DN, giving access to more groups than required by the application.

For example, you can configure `Group Base DN` values at different levels to get to the `ecmAdmin` group in this LDAP tree:

```
dc=com
  dc=oracle
    dc=us
      cn=Groups
        cn=ECM
          cn=ecmAdmin
```

Avoid using the following levels because too much of the tree would need to be queried to get the groups assigned to users:

```
dc=oracle,dc=com

dc=us,dc=oracle,dc=com

cn=groups,dc=us,dc=oracle,dc=com
```

In this case only the groups directly associated the Oracle WebCenter Content applications need to be searched:

```
cn=ECM,cn=groups,dc=us,dc=oracle,dc=com
```

You could add other groups at the Oracle WebCenter Content level so that the LDAP tree would maybe look more like this:

```
dc=com
   dc=oracle
     dc=us
       cn=Groups
         cn=ECM
           cn=ecmAdmin
           cn=ecmGuest
           cn=ecmManager
           cn=ecmSupervisor
           cn=ecmUser
```

3.10 Adding Users to Oracle Internet Directory

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

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

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

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

To add users to Oracle Internet Directory:

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

   The Create New Entry wizard starts.
4. Specify the object classes for the new entry.

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

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

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

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

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

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

8. Click **Next**.

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

9. Click **Finish**.
10. To manage optional attributes, navigate to the entry you have just created in the Data Tree.
11. If the entry is a person, click the **Person** tab and use it to manage basic user attributes.

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

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

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

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

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

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

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

3.11 Configuring Single Sign-On (SSO)

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

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

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

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

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

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

3.11.1 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 9.4, "Integrating Rights with Oracle Access Manager 11g."

For information about configuring Oracle Access Manager SSO for Imaging, see *Administering Oracle WebCenter Content: Imaging*.

Note: When you use Oracle Access Manager (OAM) WebGate 11*g* SSO with Imaging, set the following WebGate 11*g* Agent user-defined parameter:

```
filterOAMAuthnCookie=false
```

Without this parameter setting, using the Imaging viewer in advanced mode would result in an error. For more information about setting the Agent user-defined parameters, see the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*.

For information about configuring it for WebCenter Content, Inbound Refinery, or Records, see "Configuring WebCenter Content for Single Sign-On" in *Administering Oracle WebCenter Content*.

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

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

Application	Configuration Information
WebCenter Content, with Content Server	"Configuring Oracle Access Manager 11g with Oracle WebCenter Content" in *Administering Oracle WebCenter Content*
Imaging	"Integrating Oracle Access Manager 11g with Imaging" in *Administering Oracle WebCenter Content: Imaging*
Oracle IRM Web Interface	Section 9.4, "Integrating Rights with Oracle Access Manager 11g"
Oracle IRM Desktop	Not supported
Records	"Configuring Oracle Access Manager 11g with Oracle WebCenter Content" in *Administering Oracle WebCenter Content*

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

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

Application	Configuration Information
WebCenter Content, with Content Server	"Configuring Oracle Access Manager 10g with Oracle WebCenter Content" in *Administering Oracle WebCenter Content*
Imaging	"Integrating Oracle Access Manager 10g with Imaging" in *Administering Oracle WebCenter Content: Imaging*
Oracle WebCenter Enterprise Capture	Not supported
Oracle IRM Web Interface	Not supported
Oracle IRM Desktop	Section 9.4, "Integrating Rights with Oracle Access Manager 11g"
Records	"Configuring Oracle Access Manager 10g with Oracle WebCenter Content" in *Administering Oracle WebCenter Content*

3.11.2 Configuring Oracle Single Sign-On

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

Table 3–9 OSSO Configuration for Oracle WebCenter Content Applications

Application	Configuration Information
WebCenter Content, with Content Server	"Configuring Oracle Single Sign-On for WebCenter Content" in *Administering Oracle WebCenter Content*
Imaging	"Configuring Imaging and Single Sign-On for Windows Native Authentication" in *Administering Oracle WebCenter Content: Imaging*
Oracle WebCenter Enterprise Capture	Not supported
Oracle IRM Desktop	Not supported

3.11.3 Configuring Windows Native Authentication

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

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

Table 3–10 WNA Configuration for Oracle WebCenter Content Applications

Application	Configuration Information
WebCenter Content, with Content Server	"Configuring WebCenter Content and Single Sign-On for WNA" in *Administering Oracle WebCenter Content*
Imaging	"Configuring Imaging and Single Sign-On for Windows Native Authentication" in *Administering Oracle WebCenter Content: Imaging*
Oracle IRM Web Interface	"Configuring Single Sign-On with Microsoft Clients" in *Securing Oracle WebLogic Server*
Oracle IRM Desktop	"Configuring Single Sign-On with Microsoft Clients" in *Securing Oracle WebLogic Server*
Records	"Configuring Single Sign-On with Microsoft Clients" in *Securing Oracle WebLogic Server*

3.12 Integrating Oracle Web Tier with WebCenter Content

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

For information about installing and Oracle Web Tier (OHS), see "Installing and Configuring the Oracle HTTP Server" in *Administering Oracle WebCenter Portal*.

3.13 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 *Using Clusters for Oracle WebLogic Server*.

If you select **Managed Servers, Clusters, and Machines** on the Select Optional Configuration screen, you will see the screens that Table 3–11 describes.

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

Screen	Description and Action Required
Configure Managed Servers	Add new Managed Servers, or edit and delete existing Managed Servers. Click **Next** to continue.
Configure Clusters	Create clusters if you are installing in a high availability environment. For more information, see the *High Availability Guide*. Click **Next** to continue.
Assign Servers to Clusters	If you configured any clusters on the Configure Clusters screen Click **Next** to continue.
Create HTTP Proxy Applications	If you configured any clusters on the Configure Clusters screen and assigned some, but not all, of the Managed Servers in the domain to a cluster Click **Next** to continue.
Configure Machines	Configure the machines that will host the Managed Servers in a cluster. Click **Next** to continue.
Assign Servers to Machines	Assign each Managed Server to a machine. Click **Next** to continue.
Target Deployments to Clusters or Servers	Assign your Managed Servers to clusters or servers in your domain. Click **Next** to continue.
Target Services to Clusters or Servers	Use this screen to target your services (such as JMS and JDBC) to servers or clusters so that your applications can use the services. Click **Next** to continue.

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

3.14 Setting Up Oracle Web Services Manager Security

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

1. Installing Oracle WebLogic Server and Oracle WebCenter Content
2. Creating an Oracle WSM MDS Schema with the Repository Creation Utility
3. Configuring Oracle WebCenter Content Applications and Oracle WSM Policy Manager in an Oracle WebLogic Server Domain
4. Configuring the Server Socket Port and Incoming Socket Connection Address Security Filter for Oracle WSM
5. Securing Web Services with a Keystore and Oracle WSM Policies

3.14.1 Installing Oracle WebLogic Server and Oracle WebCenter Content

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

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

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

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

Metadata Services under **AS Common Schemas**

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

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

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

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

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

During postinstallation 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 postinstallation configuration of a Managed Server, see one or more of these sections:

- Section 4.3, "Completing the Initial Configuration of Content Server"
- Section 5.1, "Completing the Initial Inbound Refinery Configuration"
- Section 6.1, "Completing the Initial Imaging Configuration"
- Section 9.1, "Completing the Initial Oracle IRM Configuration"
- Section 8.1, "Completing the Initial Records Configuration"

3.14.5 Securing Web Services with a Keystore and Oracle WSM Policies

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

3.14.5.1 Setting Up a Keystore

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

The suggested location for the keystore 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 keystore in this location ensures that the keystore file is backed up when the domain and corresponding credential store files are backed up.

To set up a keystore:

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

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

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

   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 keystore, see Section 9.1.2, "Configuring a Keystore for Oracle IRM."

3.14.5.2 Applying Oracle WSM Policies to Web Services

You can use Oracle Enterprise Manager 11*g* Fusion Middleware Control to apply Oracle WSM policies to web services. For more information, see "Attaching Policies to Web Services" in the *Oracle Fusion Middleware Security and Administrator's Guide for Web Services*.

4 Completing the WebCenter Content Configuration

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

This chapter includes the following sections:

4.1 Configuring the Report Library for Records Management in Content Server

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

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

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

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

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

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

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

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

   ```
   MW_HOME/WCC_ORACLE_HOME/ucm/idc/components/ReportPublisher/lib/
   ```

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

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

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

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

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

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

   ```
   MW_HOME/WCC_ORACLE_HOME/ucm/idc/components/ServletPlugin/cs.ear
   ```

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

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

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

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

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

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

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

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

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

   c. Start the WebCenter Content Managed Server, as described in Section 10.3, "Restarting a Managed Server."

5. Start the WebCenter Content Managed Server, as described in Section 10.2, "Starting Managed Servers."

   If the Managed Server has been started before, restart it, as described in Section 10.3, "Restarting a Managed Server."

For information about adding the Records Management feature to Content Server, see Section 4.13, "Configuring Records Management in Content Server"

4.2 Completing the Initial WebCenter Content Configuration

After you start the Administration Server and Oracle WebCenter Content Managed Server, as described in Chapter 10, "Verifying the Oracle WebCenter Content Configuration," you can complete the WebCenter Content configuration on the postinstallation configuration page in Content Server.

The first user to log in to Oracle WebCenter Content Server must be the administrator of the Oracle WebLogic Server domain, to complete the configuration of Content Server. For more information, see Section 10.6, "Verifying the Configuration of Oracle WebCenter Content," and see also "Overview of System Administration Tasks," "Understanding Security and User Access," and "Managing System Processes" in *Administering Oracle WebCenter Content*.

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

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

When you configure WebCenter Content on the same machine and in the same Oracle WebLogic Server domain as Oracle Web Center Content: Imaging, the postinstallation configuration of WebCenter Content is done automatically. If you follow the default configuration for the installation of WebCenter Content and Imaging, both applications are installed on the same machine. In this environment, Imaging provides a configuration file that sets up WebCenter Content for use by Imaging.

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

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

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

To complete the WebCenter Content configuration:

1. Start the Administration Server, as described in Section 10.1, "Starting the Administration Server."

2. Start the WebCenter Content Managed Server, as described in Section 10.2, "Starting Managed Servers."

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

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

   > **Important:** The first user to log in to Oracle WebCenter Content Server must be the administrator of the Oracle WebLogic Server domain, to complete the configuration of Content Server. For more information, see Section 10.6, "Verifying the Configuration of Oracle WebCenter Content," and see also "Overview of System Administration Tasks," "Understanding Security and User Access," and "Managing System Processes" in *Administering Oracle WebCenter Content*.

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

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

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

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

   ```
   127.0.0.1|your.server.IP.address|0:0:0:0:0:0:0:1|
   ```

   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 Content Server.

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

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

For more information, see Section 3.14.4, "Configuring the Server Socket Port and Incoming Socket Connection Address Security Filter for Oracle WSM."

6. Click **Submit**.
7. Restart Content Server, as described in Section 10.3, "Restarting a Managed Server."

4.3 Completing the Initial Configuration of Content Server

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

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

For information about changing the configuration of Content Server and additional configuration options, see "Configuring System Properties" in *Administering Oracle WebCenter Content*.

4.3.1 Starting Content Server

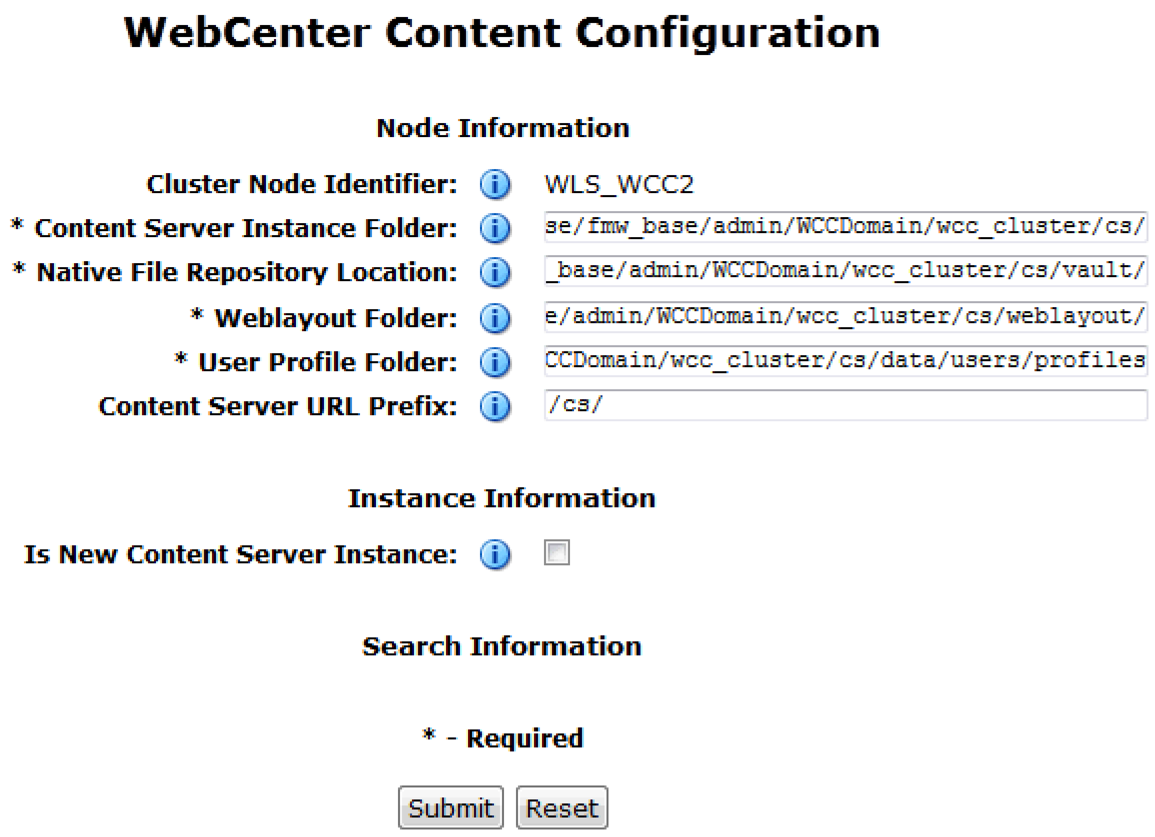
You can start WebCenter Content, which includes Content Server, with the Oracle WebLogic Server Administration Console, the `startManagedWebLogic` startup script, or Oracle Enterprise Manager Fusion Middleware Control.

For more information, see "Managing System Processes" in *Administering Oracle WebCenter Content*.

4.3.2 Configuring the Content Server Instance

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

Figure 4–1 Configuration Page for Content Server



WebCenter Content Configuration

Node Information

Cluster Node Identifier: WLS_WCC2

* Content Server Instance Folder: se/fmw_base/admin/WCCDomain/wcc_cluster/cs/

* Native File Repository Location: _base/admin/WCCDomain/wcc_cluster/cs/vault/

* Weblayout Folder: e/admin/WCCDomain/wcc_cluster/cs/weblayout/

* User Profile Folder: CCDomain/wcc_cluster/cs/data/users/profiles

Content Server URL Prefix: /cs/

Instance Information

Is New Content Server Instance: □

Search Information

* - Required

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

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

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

Field	Description
Company Mail Server	An email server that Content Server can use to send email notifications. This value generally takes the form of *`mail.example.com`*. If applicable, make sure to allow for sending email through a firewall.
Administrator E-Mail Address	An email address that Content Server can use to send email notifications (`SysAdminAddress`). This address will receive a returned message for any delivery failure that occurs.
Server Instance Name	The name of the Content Server instance. This name should contain only letters, numerals, and underscore characters. Other characters can cause problems. For example, an instance name that contains periods can cause a JavaScript error if the name is used to create a JavaScript variable.
Server Instance Label	The instance name that is displayed in the Windows **Start** menu (`InstanceMenuLabel` property).
Server Instance Description	A description of the Content Server instance (`InstanceDescription` property).
Is Auto Number Enabled	Whether or not automatic numbering of Content Server instances is enabled.
Auto Number Prefix	A unique prefix for a Content Server instance number, to avoid conflicts among multiple Content Server instances (Auto Number Prefix system property).
FullText Search Option	Specifies the search engine for full-text searches: ■ **None**: The Content Server instance will use `DATABASE.METADATA` as the search engine. ■ **Internal**: For Oracle Database 11*g*, the Content Server instance will use `OracleTextSearch` with the system database. For Microsoft SQL Server, Content Server will use `DATABASE.FULLTEXT`. For IBM DB2, Content Server will use `DATABASE.METADATA`. ■ **External**: The Content Server instance will use `OracleTextSearch` with an external data source in an Oracle Database (not the system database), SQL Server, or IBM DB2. If you select this option, you must provide the name of the external data source in the **External DataSource** field.
External DataSource	The name of an external data source that was created and targeted through the Administration Console to the WebCenter Content Managed Server, using an `OCSSEARCH` schema that was created with Repository Creation Utility (RCU). For information about an external data source, see "What You May Need to Know About JDBC Data Source for Oracle WebLogic Server" in the *Java EE Developer's Guide for Oracle Application Development Framework*. If the external data source is for use with IBM DB2, see also Section 4.3.5, "Configuring Content Server for IBM DB2 Database Searches." For information about the `OCSSEARCH` schema, see Section 2.2, "Creating Oracle WebCenter Content Schemas with the Repository Creation Utility."

4.3.3 Enabling or Disabling Components

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

To enable or disable components:

1. Log in to WebCenter Content as an administrator.
2. From the **Administration** tray or menu for your Content Server instance, choose **Admin Server**, then **Component Manager**.
3. In the first paragraph of the Component Manager page, click **advanced component manager**.
4. You can select individual components in the lists of enabled and disabled server components to view details about each component, and you can select categories of components to view. You can enable and disable components on this page, plus install and uninstall custom components.

Notes:

- If you are using Records Management with Content Server, do not disable the `ContentFolios` component, which is required for access to the Records Management web interface. This component is enabled automatically when you configure the Records Management feature.

  For more information about Records Management, see Section 4.13, "Configuring Records Management in Content Server."

- If you upgrade from Oracle WebCenter Content 11*g*R1 (11.1.1.5) to Oracle WebCenter Content 11*g*R1 (11.1.1.9.0) with the `LinkManager8` component enabled, you need to disable `LinkManager8` and enable the `LinkManager` component. `LinkManager8` was renamed to `LinkManager` in Oracle WebCenter Content 11*g*R1 (11.1.1.6).

4.3.4 Configuring the Folders Interface

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

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

To configure the folders interface:

1. Log in to WebCenter Content as an administrator.
2. From the **Administration** tray or menu for your Content Server instance, choose **Admin Server**, then **Component Manager**.

3. On the Component Manager page, select **Folders** to display the Folders category of components.
4. Select the **FrameworkFolders** component.
5. Click the **Update** button, and then click **OK** to confirm enabling the component.
6. In the first paragraph of the Component Manager page, click **advanced component manager**.
7. If **Folders_g** is in the Enabled Components box on the Advanced Component Manager page, select this component, and then click the **Disable** button.
8. Restart Content Server, as described in Section 10.3, "Restarting a Managed Server."

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

4.3.5 Configuring Content Server for IBM DB2 Database Searches

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

To configure IBM DB2 database searches in Content Server:

1. Log in to WebCenter Content as an administrator.
2. From the **Administration** tray or menu for your Content Server instance, choose **Admin Server**, then **General Configuration**.
3. Near the bottom of the General Configuration page, add the following line to the Additional Configuration Variables box:

   ```
   SSUseContains=false
   ```

4. Click **Save**.
5. Restart Content Server, as described in Section 10.3, "Restarting a Managed Server."

4.3.6 Configuring Microsoft SQL Server to Work with WebCenter Content

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

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

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

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

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

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

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

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

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

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

4.4 Configuring Additional Parameters for WebCenter Content Cluster Nodes

For WebCenter Content cluster nodes, you need to add some additional parameters to avoid performance problems such as stuck threads or other file system issues.

Using a text editor, add the following options to each cluster node's *DOMAIN_HOME*/ucm/cs/bin/intradoc.cfg file, where the directories specified are on a direct-bus-attached-controlled *local* disk and not a remote file system, such as a Windows mapped drive to NTFS/CIFS, or a UNIX/Linux mounted NFS or clustered file system (like OCFS2, GFS2, or GPFS):

```
TraceDirectory=local_domain_home/servers/UCM_serverN/logs/
EventDirectory=local_domain_home/servers/UCM_serverN/logs/event/
ArchiverDoLocks=true
DisableSharedCacheChecking=true
```

For each cluster node created with the Oracle WebLogic Scripting Tool (WLST) unpack command, you will need to create the preceding directories, ensuring that the permissions are the same as for the first installed node (RWXD for the user executing the WebCenter Content Managed Server, usually oracle). The trailing *N* should match the node's server name, like UCM_server1 is node1, UCM_server2 is node 2, and so on.

Note: The directories can reside in any local disk path that you have determined to have enough space to hold the WebCenter Content logs and any trace that you might configure. The preceding paths are suggestions.

Finally, add one more parameter, which must be on a *shared* file system (unlike the other entries, which should point to the local disk installation):

```
UserProfilesDir=ORACLE_BASE/admin/domain_name/wcc_cluster_name/cs/data/users/profiles/
```

Note: A WebCenter Content Managed Server cannot be configured for server migration.

4.5 Configuring OracleTextSearch for Content Server

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

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

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

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

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

1. Select **Internal** or **External** in the **FullText Search Option** field.
2. If you selected the **External** option, provide the name of the external data source in the **External DataSource** field.

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

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

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

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

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

   You can use the Administration Console, WebLogic Scripting Tool Command, or Fusion Middleware Control to create a data source.
3. Use the Administration Console to target the data source to the WebCenter Content Managed Server (`UCM_server1` by default).

For information about creating an external data source and targeting it to a Managed Server, see "What You May Need to Know About JDBC Data Source for Oracle WebLogic Server" in the *Java EE Developer's Guide for Oracle Application Development Framework*.

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

Note: If you plan to use the WebCenter Content user interface (described in Chapter 12, "Installing and Configuring the WebCenter Content User Interface"), you may want to optimize the `dOriginalName` field for the search index. The WebCenter Content user interface leverages the file name as its primary identifier presented in the interface. You can sort presentations by file name, which is the value of the `dOriginalName` field in Content Server.

By default, Content Server configures only the document title (`dDocTitle`) as a field available for searching and sorting. The WebCenter Content user interface, by default, does not use document titles in its displays.

The process of enabling `dOriginalName` as a new search or sort field requires a full rebuild of the fulltext index.

To configure OracleTextSearch for Content Server in the configuration file:

1. Open the *DomainHome*`/ucm/cs/config/config.cfg` file for the Content Server instance in a text editor.
2. Set the following values:

```
SearchIndexerEngineName=OracleTextSearch

IndexerDatabaseProviderName=SystemDatabase
```

Notes:

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

---

3. Save the file.
4. Restart Content Server, as described in Section 10.3, "Restarting a Managed Server."
5. Rebuild the search index using the **Indexer** tab of the **Repository Manager**, located under **Administration**, in **Admin Applets**.

For more information about rebuilding the index, see "Working with the Search Index" in *Administering Oracle WebCenter Content*.

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

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

- Patch 7446163
- Patch 6851110

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

1. Download patches 7446163 and 6851110 and print or save their Read Me documents from My Oracle Support (formerly Oracle*MetaLink*) at `https://support.oracle.com`.
2. To apply each patch, follow the instructions in its `Read Me` document.

4.5.2 Configuring an External Database Provider for Standalone Applications

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

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

4.6 Installing the Check Out and Open ActiveX Control on a Windows Client

Check Out and Open is a component of Content Server that enables users to check out and open content items in WebDAV-compliant applications directly from Content Server.

An ActiveX control is used for Internet Explorer browsers to provide the Check Out and Open functionality on Windows client computers. (A Java applet is used for other browsers, such as Firefox.) Some organizations have user environments that do not allow downloaded ActiveX controls to be installed. In addition, users in such environments might not have administrative access to their client computers. This limits the ability for individual users to install client software or allow downloaded controls to be installed.

To work around this limitation, you can manually register the `CheckOutAndOpen.dll` file on a client computer. The following instructions are for a Windows operating system.

To install the Check Out and Open ActiveX control on a Windows client:

1. Obtain the `CheckOutAndOpen.dll` file. This DLL file is located inside the *`DomainHome`*`/ucm/cs/weblayout/common/checkoutandopen.cab` file. Use a standard ZIP file tool, such as WinZip, to extract the file to a directory, such as `C:\Windows\System32`.

   You can extract the `CheckOutAndOpen.dll` file to a different directory of your choice.

2. Open a command-line console.
3. Go to the location where you extracted the `CheckOutAndOpen.dll` file; for example:

   ```
   cd \windows\system32
   ```

4. Register the DLL file with the following command:

   ```
   regsvr32 CheckOutAndOpen.dll
   ```

   You can include the silent switch, `-s`, in the `regsvr32` command.

5. At this point the ActiveX control is registered with the Windows system.

   The first time a check-out-and-open operation is attempted on the computer, the control will be enabled within the browser. Internet Explorer will attempt to first look to see if an object with the COAO CLSID is installed and use it before attempting to download the ActiveX control. The user should not be prompted to accept the installation.

You can validate that the control is registered in Internet Explorer 7 or 8 as follows:

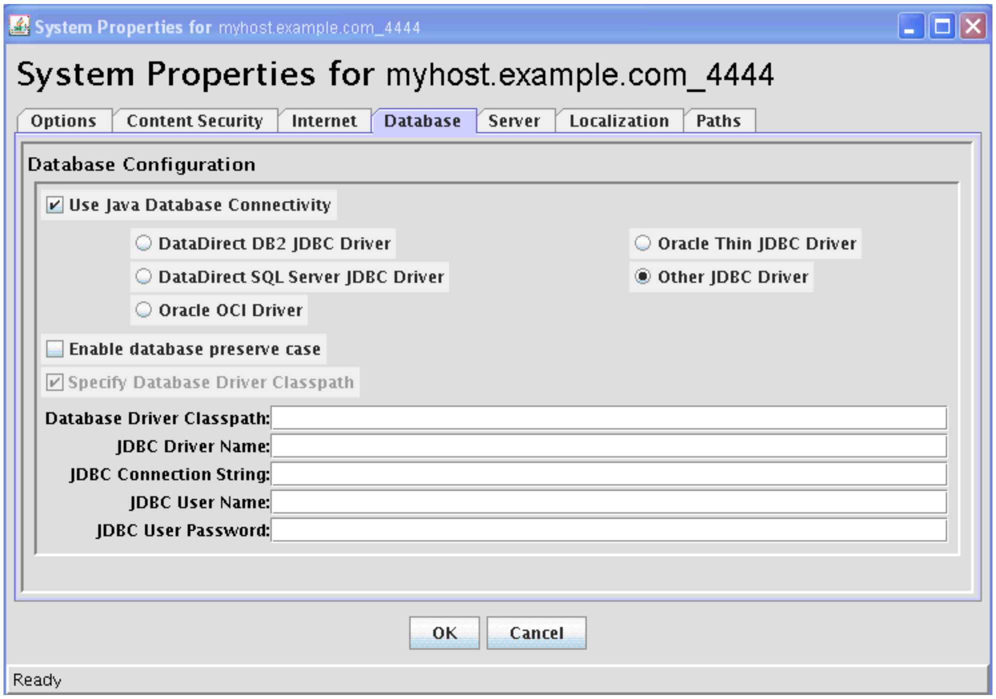
1. From the **Tools** menu, choose **Internet Options**.
2. Click the **Programs** tab.
3. Click the **Manage add-ons** button.
4. Verify that `Check Out And Open Control` is in the list of enabled add-ons.

> **Note:** If Desktop Integration Suite 7.5 or later (including 10*g*R3) is installed, it will copy a version of `CheckOutAndOpen.dll` and register it. If the Check Out and Open component is referencing the same CLSID as the one installed by Desktop Integration Suite, then this control is used rather than downloaded.

4.7 Configuring a JDBC Driver for Standalone Applications

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

Figure 4–2 System Properties Utility



System Properties for myhost.example.com_4444

Database Configuration

☑ Use Java Database Connectivity

○ DataDirect DB2 JDBC Driver
○ DataDirect SQL Server JDBC Driver
○ Oracle OCI Driver
○ Oracle Thin JDBC Driver
● Other JDBC Driver

□ Enable database preserve case

☑ Specify Database Driver Classpath

Database Driver Classpath:
JDBC Driver Name:
JDBC Connection String:
JDBC User Name:
JDBC User Password:

To configure a JDBC Driver for standalone applications:

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

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

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

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

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

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

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

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

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

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

4. Enter the user name and password for the database in the **JDBC User Name** and **JDBC User Password** fields.
5. Click **OK**.
6. Restart Content Server, as described in Section 10.3, "Restarting a Managed Server."

4.8 Importing a Database Root CA Certificate into the Keystore for a Standalone Application

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

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

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

1. Import the certificate into the standard Java keystore 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_version\bin\keytool -import -trustcacerts
     -alias dbroot -keystore
   c:\mw_home\jrockit_version\jre\lib\security\cacerts -storepass
     changeit -file b64certificate.txt
   ```

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

   For example:

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

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

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

4.9 Enabling and Configuring Site Studio on Content Server

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

- **Site Studio**, which uses Site Studio Designer to create websites

  This version requires that the SiteStudio component be enabled on Content Server. For more information, see Section 4.9.1, "Enabling Site Studio on Content Server."

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

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

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

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

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

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

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

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

- Enabling Site Studio on Content Server
- Setting Default Project Document Information
- Setting Default Metadata for Website Assets
- Configuring Zone Fields
- Enabling JavaServer Pages on Content Server
- Rebuilding the Content Server Index

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

You can create an 11*g* Site Studio site running on Oracle WebLogic Server and use an Oracle Universal Content Management (Oracle UCM) 10*g*R3 server as the back end. For information about using Site Studio 11*g*R1 (11.1.1.7.0) with Oracle UCM 10*g*R3, see "Configuring Oracle Content Server 10gR3 for Use with Site Studio 11gR1" in the *Technical Reference Guide for Site Studio*.

4.9.1 Enabling Site Studio on Content Server

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

To enable Site Studio on Content Server:

1. Log in to WebCenter Content as an administrator.
2. In the Content Server **Administration** tray or menu, choose **Admin Server**, then **Component Manager**.

3. 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 JDeveloper.

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

5. Restart Content Server, as described in Section 10.3, "Restarting a Managed Server."

4.9.2 Setting Default Project Document Information

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

To set the default project document information:

1. Log in to Content Server as an administrator.

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

   The Site Studio Administration page is displayed.

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

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

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

   This button returns you to the Site Studio Administration page.

4.9.3 Setting Default Metadata for Website Assets

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

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

4.9.4 Configuring Zone Fields

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

Make sure that the `DBSearchContainsOpSupport` component is enabled on Content Server. This component ensures that the zone fields are full-text indexed, which is required for Site Studio sites to work correctly. If this component is not enabled, you should enable it with the Component Manager, as described in Section 4.9, "Enabling and Configuring Site Studio on Content Server."

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

To configure Site Studio metadata fields as zone fields:

1. Log in to WebCenter Content as an administrator.
2. In the Content Server **Administration** tray or menu, choose **Zone Fields Configuration**.
3. On the Zone Fields Configuration page, select **Web Sites** and **Exclude From Lists** as zone text fields.

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

4.9.5 Enabling JavaServer Pages on Content Server

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

Important:

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

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

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

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

To configure JSP Support for a new JSP group:

1. Log in to WebCenter Content as an administrator.
2. In the **Administration** tray or menu, choose **Site Studio Administration**.
3. On the Site Studio Administration page, click **Manage Fragment Libraries**.
4. Click the **Configure JSP Support** button.

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

4.9.6 Rebuilding the Content Server Index

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

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

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

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

For more information on rebuilding the index, see "Configuring the Search Index" in *Administering Oracle WebCenter Content*.

4.10 Configuring Content Server for Desktop

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

- `DesktopIntegrationSuite`
- `DesktopTag`
- `FolderStructureArchive`
- `FrameworkFolders`

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

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

To configure Content Server for Desktop:

1. Log in to WebCenter Content as an administrator.
2. In the Content Server **Administration** tray or menu, choose **Admin Server**, then **Component Manager**.
3. On the Component Manager page, select **Folders** to display the Folders category of components.
4. Select the **FrameworkFolders** component.

5. Select the **DesktopIntegrationSuite**, **DesktopTag**, and optionally, the **EmailMetadata** components.
6. Click the **Update** button, and then click **OK** to confirm your selections.
7. In the first paragraph of the Component Manager page, click **advanced component manager**.
8. In the Disabled Components box on the Advanced Component Manager page, select **FolderStructureArchive**, and click the **Enable** button.
9. If **Folders_g** is in the Enabled Components box, select this component, and click the **Disable** button.
10. Make sure that the `CoreWebdav` component is enabled:
    a. Under Category Filters on the Advanced Component Manager page, select **Show System Components**.
    b. If **CoreWebdav** is not in the Enabled Components box, select **CoreWebdav** in the Disabled Components box, and click the **Enable** button.
11. Restart Content Server, as described in Section 10.3, "Restarting a Managed Server."

4.11 Installing and Configuring Desktop on a Client Workstation

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

For information about how to install Desktop on a client workstation, see "Setting Up the Desktop Client Software on Your Computer" in *Using Oracle WebCenter Content: Desktop*.

4.12 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 website at

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

4.13 Configuring Records Management in Content Server

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

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

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

To configure Records Management in Content Server:

1. From the **Administration** tray or menu, choose **Configure Records Settings** to go to the Records Management Setup Checklist, then click **Configure Installation**.
2. On the Enabled Features page, select a Records Management option for which you are licensed:
   - **None**
   - **Standalone**
   - **Adapter**
3. Click **Submit**.
4. Restart WebCenter Content, as described in Section 10.3, "Restarting a Managed Server."

   Whenever the screen says to restart the server during the Records Management configuration, restart the WebCenter Content Managed Server.
5. After you restart WebCenter Content, the Records Management Setup Checklist is displayed again.

   For information about completing items on the Setup Checklist, see Section 8.1.2, "Completing the Setup Checklist for Records."
6. If you selected **Adapter**, click **Register Source** on the Enabled Features page, and then supply values for the fields on the Register Source page:
   - **Provider Name:** Specify the outgoing provider used to connect to the Records Managed Server. You can choose from the list of current outgoing providers, or you can click the **Add** button and create one yourself. The provider dialog box shows an abbreviated list of provider fields.

     You can also add providers from the regular Providers page. To view information about an existing provider, click **Info** in the **Action** column.
   - **Source Name:** Specify the name of the external source to be added to the Records Managed Server. The source name is required and cannot contain spaces.
   - **Source Table Name:** Specify the prefix to use for creating database tables. If this value is not specified, it is defaulted to the source name.
   - **Source Display Name:** Specify the caption to use for displaying the source name. If this value is not specified, it is defaulted to the source name.

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

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

- Validate the provider and test the connection to the Records Managed Server
- Validate the specified source values

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

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

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

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

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

   - Configure Custom Fields

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

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

     * Add an external custom field.
     * Edit an external custom field.
     * Configure the disposition actions.
     * Configure the scheduled events.
     * View the external source information (from the **Info** menu, select **Source Information**).

   - Configure Scheduled Times

     The Configure Scheduled Times page enables you to specify when the scheduled tasks are to run. You can specify the interval at which the tasks are run (in hours, days, or weeks) and the time of day. This enables you to schedule the tasks at times when there might be less activity.

8. After Records Management is initially configured on Content Server, the menu bar includes a **Records** menu. You can change the Records Management configuration through options on this menu.

   For more information about configuring Records Management, see *Managing Oracle WebCenter Content*.

9. From the **Records** menu, select **Configure** and then **Enabled Features**.

   On the Enabled Features page, you can change the selection of features and dispositions. For the adapter, the features you select cannot be more than the features selected on the Records server. For more information about the Features and Disposition Actions sections of the Enabled Features page, see Section 8.1.1, "Configuring the Level of Records Features."

   After you change any features or dispositions, restart WebCenter Content, as described in Section 10.3, "Restarting a Managed Server."

4.14 Configuring Oracle iPlanet Web Server As a Web Tier for Oracle WebCenter Content

You can configure the Oracle iPlanet Web Server as a web tier for Oracle WebCenter Content. For more information, see the "Configuring the iPlanet as web tier for Oracle WebCenter Content" blog.

4.15 Configuring Shared Folders for WebCenter Content Clustering

If you are using a cluster of WebCenter Content Managed Servers, you need to configure a shared file system for the WebCenter Content cluster. For more information, see the "WebCenter Content shared folders for clustering" blog.

4.16 Installing and Configuring AXF for BPM and AXF for BPEL

Oracle WebCenter Content: AXF for BPM and Oracle Application Extensions Framework (AXF) for BPEL are installed automatically with Imaging. Before you can configure AXF for BPM or AXF for BPEL in a WebLogic Server domain with Imaging, you need to create an AXF schema with the Repository Creation Utility, as described in Section 2.2.2, "Creating Schemas for Oracle WebCenter Content Applications." You can select AXF for BPM to it to the Imaging Managed Server when the domain is created or extended, as described in Chapter 3, "Configuring Oracle WebCenter Content Applications." AXF for BPEL is deployed as part of the Imaging application.

For information about AXF for BPM or AXF for BPEL installation, configuration, and verification with Imaging, see Section 6.5, "Installing and Configuring AXF for BPM and AXF for BPEL."

For additional information about configuring and using AXF for BPM or AXF for BPEL and the AXF for BPEL database tables (Imaging tables), see *Administering the Application Adapters for Oracle WebCenter*.

5 Completing the Inbound Refinery Configuration

This chapter explains how to complete the initial configuration of Oracle WebCenter Content: Inbound Refinery in an Oracle WebLogic Server domain.

This chapter includes the following sections:

- Section 5.1, "Completing the Initial Inbound Refinery Configuration"
- Section 5.2, "Installing and Configuring Inbound Refinery on WebCenter Content"

5.1 Completing the Initial Inbound Refinery Configuration

Before you can use Inbound Refinery with Oracle WebCenter Content, you need to complete the configuration of Inbound Refinery for document and image conversions to work with Content Server.

For transformations to work on some platforms, certain environment variables must be set before you start the Managed Server. On a UNIX operating system running XWindows, to redirect the display to a system with suitable graphic capabilities, you need to export DISPLAY to a valid X Server before starting the Inbound Refinery Managed Server. For more information, see Section 3.7.2, "Setting Library Paths in Environment Variables on UNIX Platforms."

To complete the Inbound Refinery configuration:

1. Start the Administration Server and the Inbound Refinery and WebCenter Content Managed Servers, as described in Chapter 10, "Verifying the Oracle WebCenter Content Configuration."

2. Configure Content Server, as described in Section 4.2, "Completing the Initial WebCenter Content Configuration."

3. Browse to the Inbound Refinery postinstallation configuration page, at this website:

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

4. Enter or edit all necessary values.

   - To enable access from Content Server, provide a value for **Incoming Socket Connection Address Security Filter**, as follows:

     ```
     127.0.0.1|0:0:0:0:0:0:0:1|your.server.IP.address
     ```

     This value should be the IP address of the Content Server instance or instances that will send jobs to Inbound Refinery, not the IP address of Inbound Refinery. (In a test or demo environment, these IP addresses could be the same.)

     This field accepts wildcards in the value, like `10.*.*.*`. You can change this value later by setting `SocketHostAddressSecurityFilter` in `*DomainHome*/ucm/ibr/config/config.cfg` and restarting Inbound Refinery.

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

   - In the **Server Socket Port** field, you must enter an unused port number, such as `5555`, to set up a provider from Content Server to Inbound Refinery.

     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`. The default `IntradocServerPort` value is 5555.

     Notes:

     - The **Server Socket Port** value must be set correctly for Inbound Refinery to be usable.
     - The default port number is `5555` for Oracle WebLogic Server Node Manager and for Inbound Refinery. If both will run on the same server, you need to configure a different port number for Inbound Refinery or Node Manager.

5. Restart Inbound Refinery, 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 Inbound Refinery configuration.

   Note: An Inbound Refinery Managed Server cannot be configured for server migration.

5.2 Installing and Configuring Inbound Refinery on WebCenter Content

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

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

- Configuring Inbound Refinery on WebCenter Content
- Configuring Document Conversion in Inbound Refinery
- Setting Up Content Server to Send Jobs to Inbound Refinery for Conversion
- Changing the Path to the Font Directory for Inbound Refinery (Optional)

5.2.1 Configuring Inbound Refinery on WebCenter Content

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

To configure Inbound Refinery on WebCenter Content:

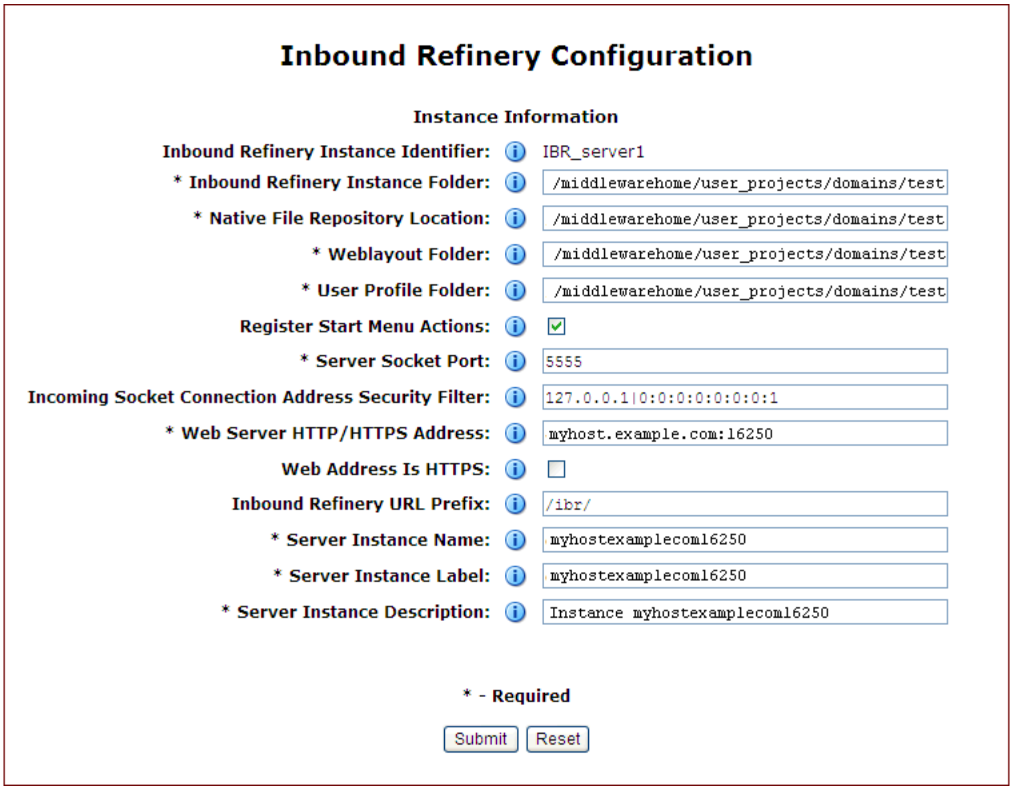
1. Configure Content Server, as described in Section 4.3, "Completing the Initial Configuration of Content Server."

2. Browse to the Inbound Refinery postinstallation configuration page, at this website:

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

   Figure 5–1 shows the Inbound Refinery Configuration page for postinstallation configuration.

Figure 5–1 Inbound Refinery Configuration Page



Inbound Refinery Configuration

Instance Information

Inbound Refinery Instance Identifier:	IBR_server1
*** Inbound Refinery Instance Folder:**	/middlewarehome/user_projects/domains/test
*** Native File Repository Location:**	/middlewarehome/user_projects/domains/test
*** Weblayout Folder:**	/middlewarehome/user_projects/domains/test
*** User Profile Folder:**	/middlewarehome/user_projects/domains/test
Register Start Menu Actions:	☑
*** Server Socket Port:**	5555
Incoming Socket Connection Address Security Filter:	127.0.0.1|0:0:0:0:0:0:0:1
*** Web Server HTTP/HTTPS Address:**	myhost.example.com:16250
Web Address Is HTTPS:	□
Inbound Refinery URL Prefix:	/ibr/
*** Server Instance Name:**	myhostexamplecom16250
*** Server Instance Label:**	myhostexamplecom16250
*** Server Instance Description:**	Instance myhostexamplecom16250

*** - Required**

3. Enter or edit all necessary values.

   The following table describes the field values on the Inbound Refinery Configuration page, where the required values are marked with asterisks, as Figure 5–1 shows.

Field	Description
Inbound Refinery Instance Folder	The absolute path to the Oracle instance directory of Inbound Refinery, which is *DomainHome*/ucm/by default. The default Oracle instance directory for Inbound Refinery follows: `MW_HOME/user_projects/domains/DomainHome/ucm/ibr` The name of the top-level folder in the folder hierarchy for the Content Server instance is `ibr`. The path to the Oracle instance directory is the value of the `IntradocDir` variable for the Inbound Refinery instance. This directory path should be unique to this particular Managed Server, or node. For installations that are likely to be upgraded to future versions of the product, Oracle strongly recommends that you change the location of the Oracle instance directory to a directory outside of any Oracle WebLogic Server domain directories or installation directories.
Native File Repository Location	The directory where conversion jobs are stored while they are being processed. After a job is converted and picked up by Content Server, the job is removed from this directory. You do not need to change this path.
Weblayout Folder	The URL for the Inbound Refinery web interface. You do not need to change this path.
Register Start Menu Actions	Whether or not the **Start Menu** actions will be registered.
Server Socket Port	The number of the port for calling top-level services. To set up a provider from Inbound Refinery back to Content Server, you can leave the default **Server Socket Port** value, `5555`, or change it to an unused port number. Changing this field value changes the `IntradocServerPort` entry in *DomainHome*/ucm/ibr/config/config.cfg. **Notes:** ■ The **Server Socket Port** value must be set correctly for Inbound Refinery to be usable. ■ The default port number is `5555` for Oracle WebLogic Server Node Manager as well as for Inbound Refinery. If both will run on the same server, you need to configure a different port number for Inbound Refinery or Node Manager.

Field	Description
Incoming Socket Connection Address Security Filter	Restricts Inbound Refinery access to a computer or computers with a specified IP address or addresses. To enable access from Content Server, provide a value for this field as follows: `127.0.0.1|0:0:0:0:0:0:0:1|`*`your.server.IP.address`* This value should be the IP address of the Content Server instance or instances that will send jobs to Inbound Refinery, not the IP address of Inbound Refinery. (In a test or demo environment, these IP addresses could be the same.) This field accepts wildcards in the value, like `10.*.*.*`. You can change this value later by setting `SocketHostAddressSecurityFilter` in *`DomainHome`*`/ucm/ibr/config/config.cfg` and restarting Inbound Refinery. **Note:** The **Incoming Socket Connection Address Security Filter** value must be set correctly for Inbound Refinery to be usable.
Web Server HTTP/HTTPS Address	The name of the web server. (`HttpServerAddress` property).
Web Address Is HTTPS	Whether or not the URL for the web server starts with `HTTPS`, for a server that has SSL enabled.
Inbound Refinery URL Prefix	The relative URL for the Inbound Refinery instance.
Server Instance Name	The name of the Inbound Refinery instance.
Server Instance Label	The instance name that is displayed for Inbound Refinery.
Server Instance Description	A description of the Inbound Refinery instance.

4. Restart Inbound Refinery, as described in Section 10.3, "Restarting a Managed Server."

5. Restart Content Server.

   You can restart a Content Server instance by restarting the WebCenter Content Managed Server, with the Oracle WebLogic Server Administration Console, shutdown and startup scripts, or Oracle Enterprise Manager Fusion Middleware Control. For more information, see Section 10.3, "Restarting a Managed Server."

After you restart the WebCenter Content Managed Server, you can set up Inbound Refinery and Content Server for document conversion. The core Inbound Refinery uses Oracle Outside In Technology to convert native documents to web-viewable PDF files or JPEG thumbnails. Other conversions require additional Inbound Refinery components. These components are installed but disabled on Inbound Refinery by default. Some of these components are only for running on Windows operating systems, some require additional configuration, and some require certain components to be enabled on Content Server.

For Inbound Refinery to work properly, it must have access to the fonts it needs to generate images. By default, the font path is set to the font directory in the JDK used by Inbound Refinery: `java.home/lib/fonts`. However, the fonts included in the default directory are limited and might cause poor renditions. Also, if a nonstandard JDK is used, then the JDK font path may be different than that specified as the default. In these cases, you might need to change the font path to improve the quality of the renditions or to provide the correct path to the font directory in the JDK. For more information, see Section 5.2.4, "Changing the Path to the Font Directory for Inbound Refinery."

On Content Server, you must set up an outgoing provider from Content Server to Inbound Refinery, with the **Handles Inbound Refinery Conversion Jobs** option checked, as described in Section 5.2.3.1, "Creating an Outgoing Provider." You also need to enable any components that you need for your conversion types. The `InboundRefinerySupport` component is enabled by default on a new Content Server instance. If this component is not enabled, you must enable it on any Content Server instance that will use Inbound Refinery for document conversion, as described in Section 5.2.2.1, "Enabling Conversion Components in Inbound Refinery."

5.2.2 Configuring Document Conversion in Inbound Refinery

To configure document conversion in Inbound Refinery, perform these tasks:

- Enabling Conversion Components in Inbound Refinery
- Enabling PDFExportConverter in Inbound Refinery

Note: Oracle WebCenter Content Inbound Refinery supports using Microsoft Office Suite 32-bit installations for the greatest compatibility. Using 64-bit installations of Microsoft Office Suite is not supported. Microsoft Office Suite 32-bit is the default installation and is recommended by Microsoft for compatibility with third-party extensions. For more information, visit `http://office.microsoft.com` and search for articles HA010369476, HA102840825, and ee681792.

For additional information, see "Native Applications Requirements for Content Conversions" in *Oracle Fusion Middleware Managing Oracle WebCenter Content*.

5.2.2.1 Enabling Conversion Components in Inbound Refinery

The core Inbound Refinery converts files to TIFF web-viewable files and JPEG image thumbnails. To use additional conversion types, you will need to enable the necessary components.

For information about the conversion components, see "Configuring the Content Server Refinery Conversion Options" in *Managing Oracle WebCenter Content*.

To enable conversion components in Inbound Refinery:

1. From the Inbound Refinery **Administration** menu, choose **Admin Server**, then **Component Manager**.
2. On the Component Manager page, select the components you want.
3. Click **Update**.

4. Click **OK** to enable the components.
5. Restart Inbound Refinery, as described in Section 10.3, "Restarting a Managed Server."

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

5.2.2.2 Enabling PDFExportConverter in Inbound Refinery

PDFExportConverter uses Outside In Technology to convert documents directly to PDF files. The conversion can be cross-platform and does not require any third-party product. You can enable PDFExportConverter for Inbound Refinery as a server feature.

To enable PDFExportConverter on Inbound Refinery:

1. From the Inbound Refinery **Administration** menu, choose **Admin Server**, then **Component Manager**.
2. On the Component Manager page select **PDFExportConverter**, and click the **Update** button.
3. Click **Update**.
4. Click **OK** to enable this feature.
5. Restart Inbound Refinery, as described in Section 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 *Managing Oracle WebCenter Content*.
7. Make sure that file formats are configured on Content Server to be sent to Inbound Refinery, as described in Section 5.2.3.3, "Selecting File Formats To Be Converted."

5.2.3 Setting Up Content Server to Send Jobs to Inbound Refinery for Conversion

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

- Creating an Outgoing Provider
- Enabling Components for Inbound Refinery on Content Server
- Selecting File Formats To Be Converted

5.2.3.1 Creating an Outgoing Provider

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

To create an outgoing provider:

1. From the Content Server **Administration** menu, choose **Providers**.
2. In the Create a New Provider section of the Providers page, click **Add** in the **outgoing** row.

3. Enter values for these fields:

   - **Provider Name:** Any short name with no spaces. It is a good idea to use the same value as the **Instance Name** value
   - **Provider Description:** Any text string.
   - **Server Host Name:** The name of the host machine where the Inbound Refinery instance is running, such as `myhost.us.example.com`.
   - **HTTP Server Address:** The address of the Inbound Refinery instance, such as `myhost.example.com:16250`.
   - **Server Port:** The value that was entered in the **Server Socket Port** field (`IntradocServerPort` value) for the Inbound Refinery instance. This value is the number of the port for calling top-level services.

     You can find this value on the Inbound Refinery configuration information page, as follows:

     a. From the Inbound Refinery **Administration** menu, select **Configuration Information**.

     b. Next to **Server Name**, click **Server Configurations**.

     c. Look for the value for **Server Port**.
   - **Instance Name:** The instance name for Inbound Refinery (the `IDC_Name` value in the **config.cfg** file).

     This value was entered on the postinstallation configuration page for **Server Instance Name**.

     You can also find this value on the Inbound Refinery configuration information page, as follows:

     a. From the Inbound Refinery **Administration** menu, select **Configuration Information**.

     b. Look for the **Server Name**, value.
   - **Relative Web Root**: The web root of the Inbound Refinery instance, `/ibr/`.

4. Under Conversion Options, check **Handles Inbound Refinery Conversion Jobs.**

   Do *not* check **Inbound Refinery Read Only Mode**.

5. Click **Add**.

6. Restart Content Server, as described in Section 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 Content Server and Inbound Refinery instances can ping each other.

For more information about setting up providers, see "Configuring Content Server and Refinery Communication" in *Managing Oracle WebCenter Content*.

5.2.3.2 Enabling Components for Inbound Refinery on Content Server

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

To enable components for Inbound Refinery on Content Server:

1. From the Content Server **Administration** tray or menu, choose **Admin Server**, then **Component Manager**.
2. Under Inbound Refinery on the Component Manager page, select the components that you want to enable.
3. Click **Update**.
4. Restart Content Server, as described in Section 10.3, "Restarting a Managed Server."

5.2.3.3 Selecting File Formats To Be Converted

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

To select file formats to be converted:

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

   Content Server displays the File Formats Wizard page. This page configures what file formats will be sent to Inbound Refinery for conversion when they are checked into Content Server.
2. Select the formats you want converted.
3. Click **Update**.

You can also select file formats with the Configuration Manager, with more fine-grained control, including file formats that wizard does not list. For more information, see "Working with Conversions" in *Managing Oracle WebCenter Content*.

5.2.4 Changing the Path to the Font Directory for Inbound Refinery

The default font path for Inbound Refinery is the font directory in the JVM, `java.home/lib/fonts`. You might need to change the path, in some cases, to improve the quality of renditions or to specify the correct path to the font directory in a nonstandard JDK.

If the JDK font path is different from the default font path, an error message is displayed from both Inbound Refinery and Content Server. If you receive an error message, ensure that the font path is set to the directory containing the fonts necessary to properly render your conversions. If the native file contains custom fonts or non-western European characters, Inbound Refinery must have access to these fonts.

To change the path to the font directory for Inbound Refinery:

1. Log in to Inbound Refinery.
2. From the **Administration** tray or menu, choose **Conversion Settings**, then **Third-Party Application Settings**.
3. Click **Options** under General OutsideIn Filter Options.
4. Replace the path to the font directory on the General OutsideIn Filter Option page.
5. Click **Update**.

6 Completing the Imaging Configuration

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

This chapter includes the following sections:

- Section 6.1, "Completing the Initial Imaging Configuration"
- Section 6.2, "Configuring the Full-Text Features in the WebCenter Content Repository"
- Section 6.3, "Setting Imaging System Security"
- Section 6.4, "Configuring the Imaging Viewer Cache"
- Section 6.5, "Installing and Configuring AXF for BPM and AXF for BPEL"

6.1 Completing the Initial Imaging Configuration

Before you complete the configuration of Imaging, your system needs to have Oracle WebCenter Content installed and configured. Imaging uses WebCenter Content for its repository.

Your Imaging system will use WebCenter Content 11*g* as its document repository. For information about configuring WebCenter Content 11*g*, see Chapter 3, "Configuring Oracle WebCenter Content Applications," Chapter 4, "Completing the WebCenter Content Configuration," and Section 6.1.1.1, "Configuring WebCenter Content 11g to Work with Imaging."

> **Note:** In a production system, Oracle WebCenter Content applications need to use an external Lightweight Directory Application Protocol (LDAP) authentication provider rather than the Oracle WebLogic Server embedded LDAP server, which is part of the default configuration. If you want to reassociate the identity store for Imaging with an external LDAP authentication provider, it is easier to do this before you complete the configuration of the Imaging Managed Server and before you connect it to the WebCenter Content 11*g* repository. For more information, see Section 3.9, "Reassociating the Identity Store with an External LDAP Authentication Provider."

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

If a value is specified in the `DefaultSecurityGroup` MBean before Imaging security is initialized, then when the first user logs in, the specified group is given full administrative permissions as well as the user logging in.

To complete the Imaging configuration, you need to perform all of the following tasks that apply to your system:

1. Configuring a WebCenter Content Repository for Imaging
2. Starting the Administration server and the WebCenter Content Managed Server, as described in Chapter 10, "Verifying the Oracle WebCenter Content Configuration"
3. Starting the Imaging Managed Server and Accessing the Web Client
4. Connecting to a WebCenter Content Repository
5. Connecting to a Workflow Server
6. Configuring the GDFontPath MBean for a UNIX System
7. Setting DISPLAY for the Imaging Viewer in a UNIX Exalogic Environment with Solaris 11g
8. Importing Definitions

6.1.1 Configuring a WebCenter Content Repository for Imaging

You can configure WebCenter Content 11*g* as the repository for Imaging.

> **Note:** You will not be able to import or upload content to the Imaging system unless you have created a repository connection.

6.1.1.1 Configuring WebCenter Content 11g to Work with Imaging

WebCenter Content 11*g* is installed with Oracle WebCenter Content. When a WebCenter Content Managed Server and Imaging Managed Server are configured in an Oracle WebLogic Server domain on the same host machine, the configuration of WebCenter Content 11*g* to work with Imaging is automatic.

If WebCenter Content is installed in a domain that is later extended with Imaging, then WebCenter Content will not be reconfigured to work with Imaging until the next restart of the WebCenter Content Managed Server. In this case, you must restart WebCenter Content, as described in Section 10.3, "Restarting a Managed Server," before connecting to Oracle WebCenter Content Server from the Imaging web client, as described in Section 6.1.3, "Connecting to a WebCenter Content Repository."

If the WebCenter Content and Imaging Managed Servers are configured to run on different machines, configuring Imaging will not configure WebCenter Content to work with it. In this case, you must follow the manual configuration steps to configure WebCenter Content.

To configure WebCenter Content 11g manually to work with Imaging:

1. Start the WebCenter Content Managed Server, as described in Section 10.2, "Starting Managed Servers."
2. Access Content Server, as described in Section 4.3.1, "Starting Content Server."

3. Enable the `IpmRepository` component:

   a. Choose **Admin Server** from the **Administration** tray or menu, then **Component Manager**.

   b. On the Component Manager page, select **Integration.**

   c. Select **IpmRepository**, and click the **Update** button.

      This option is selected by default if the Oracle WebLogic Server domain was configured with Fusion Middleware Configuration Wizard. If this option is already selected, you can close the Component Manager without clicking **Update** or restarting Content Server.

   d. Click the **OK** button to enable this feature.

   e. Restart Content Server, as described in Section 10.3, "Restarting a Managed Server."

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

6.1.1.2 Configuring a File Store Provider for Content Storage

An administrator can configure a file store provider in Content Server 11*g* to control how and where files are stored and managed within Content Server. Instead of storing all content on a single file system, you can use a file store provider to store content across multiple file systems as well as within a database. The File Store Provider component is installed and enabled by default with WebCenter Content installation and configuration.

For Imaging, you should add a file store provider to use instead of the default file store provider. Also, you should disable the traditional web layout functionality for the file store.

You can configure a file store provider for Oracle Database.

If your WebCenter Content installation uses a Microsoft SQL Server or IBM DB2 database, do not configure a file store provider. If you are configuring a WebCenter Content Managed Server with one of these databases, you need to disable the file store provider that is enabled by default for Content Server.

For more information, see "Managing a File Store System" in *Administering Oracle WebCenter Content*.

6.1.1.2.1 Configuring a File Store Provider A file store provider can be a combination of any media supported by Content Server. Because the document storage location is not defined by the media being used for storage, the term *volume* is used to represent a storage location when an application is defined in the Imaging user interface. Imaging connects to a volume defined and configured in Content Server by an administrator. You cannot use Imaging to create or define a volume.

A Content Server administrator can configure a file store provider. For more information, see "Configuring the File Store Provider" in *Administering Oracle WebCenter Content*.

6.1.1.2.2 Disabling Web Layout Functionality for Imaging Content Server traditionally uses a `weblayout/` directory on a file system to store content in a format for viewing in a web browser, even if the main storage volume is set up in a database. This file system store is useful for making content retrieval faster for a website or for storing a secondary file that describes the primary content item, but it does not have much use in an Imaging solution. Files copied to a `weblayout/` directory in an exclusively Imaging solution would never get used, taking up unnecessary storage space. Oracle recommends disabling the web layout functionality for any file store provider that is configured for use as an Imaging volume.

Caution: If your Imaging system will use redactions, do not implement Web Layout. Users might be able to see an unredacted version of a document in the `weblayout/` directory if Web Layout (IBR) is turned on in an Imaging file store provider.

An administrator can disable the web layout functionality by selecting the **Is Webless File Store** option on the Add/Edit Storage Rule page for a file store provider in Content Server. For more information, see "Adding or Editing a Storage Rule" in *Administering Oracle WebCenter Content*.

6.1.2 Starting the Imaging Managed Server and Accessing the Web Client

After you start the Administration server and the Imaging and WebCenter Content Managed Servers, you can access the Imaging web client.

To access the Imaging web client:

1. Start the Imaging Managed Server, as described in Section 10.2, "Starting Managed Servers."

Note: If Oracle WebCenter Content: AXF for BPM is deployed to the domain, proceed to Section 6.5.1, "Configuring and Verifying AXF for BPM," before performing any configuration on the Imaging server.

---

2. Access the web client at this URL: `http://`*`managedServerHost`*`:16000/imaging`

   Log in with the administrator user name and password.

Note: This first user to connect to the Imaging system is registered as the Imaging administrator.

6.1.3 Connecting to a WebCenter Content Repository

Before Imaging can use the WebCenter Content repository, you need to configure a connection to Content Server. You can create a connection to it from Imaging.

To connect to a WebCenter Content repository:

1. Open a web browser, and navigate to this website:

   `http://`*`managedServerHost`*`:16000/imaging`

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

3. Navigate to the **Manage Connections** tray, and choose **Create Content Server Connection** from the list.
4. Enter a name for the connection on the Basic Information page and, optionally, a description, and then click **Next**.
5. You can change the selections and on the Connection Settings page:
   - **SSL:** Selected for secure SSL communications
   - **Server Port:** The IDC port of the WebCenter Content instance, `4444` for Imaging by default
   - **Use Local Content Server:** Selected by default if Content Server is on the same machine as the Imaging server.

     If the servers are not installed on the same machine, you will need to configure the Content Server machine name as part of the Content Server Pool.
6. Click **Next**.
7. Enter a **Connection Security** value for the connection.

   Select which users and groups should have permission to access, modify, delete, or grant others access to this connection definition. At least one user or group must have the grant access permission.
8. Click **Next**.
9. At the Summary screen, click **Submit**.

6.1.4 Connecting to a Workflow Server

A connection to a workflow server (Oracle SOA Suite) is required before you import the definition files. This connection will be necessary for your solution to retrieve your task list. Imaging connects to a workflow server when application fields are mapped to workflow payload elements.

To connect, the provider, port, and credential information is passed using Web Services Inspection Language (WSIL). WSIL uses the HTTP protocol and a specific XML format to allow for the discovery of the web service end points on a server. Imaging follows links in the WSIL that meet certain criteria to discover deployed composites.

The connection can be to an Oracle Business Process Management (Oracle BPM) or Business Process Execution Language (BPEL) server. For Imaging to take advantage of BPM and Oracle BPEL Process Manager within an existing domain, the domain must be extended with **Oracle BPM Suite - 11.1.1.0**. When Oracle BPM Suite was installed, it automatically selected **Oracle SOA Suite - 11.1.1.0** as its dependency. If you want to use Oracle BPEL Process Manager and not Oracle BPM, you can extend the domain with an Oracle SOA Suite installation and configuration. For more information about the installation and configuration steps for Oracle SOA Suite and Oracle BPM, see the *Installation Guide for Oracle SOA Suite and Oracle Business Process Management Suite*.

The following procedures describes how to configure a connection to a workflow server and register the connection in your database. For additional information, see "Creating a Workflow Connection" in *Administering Oracle WebCenter Content: Imaging*.

6.1.4.1 Configuring a Connection to a Workflow Server

If you installed the Oracle SOA Suite for use with Imaging (noted in Section 2.4, "Using the Installer for Oracle WebCenter Content"), such as for AXF for BPM or AXF for BPEL, you need to configure a connection to a workflow server.

To configure a connection to a workflow server:

1. Open a web browser, and navigate to this website:

   `http://managedServerHost:16000/imaging`
2. Log in with the administrator user name and password.
3. Navigate to the **Manage Connections** tray, and choose **Create Workflow 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. Optionally, change one or more of the following selections on the Connection Settings page:
   - **HTTP Front End Address**: The front end address of the workflow server, including the listening port, which is `http://<server>:8001` for Oracle SOA Suite by default.
   - **Credential Alias**: The credential store key for obtaining user and password credentials for the workflow server.
   - **Provider**: The provider setting can be either the host name or IP address of a single machine, or a comma-separated list of host names or IP addresses for multiple machines in a cluster. The listening port and transport mechanism should be included in the setting.
6. Click **Test Connection** to verify the settings.
7. Click **Next**.
8. 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.
9. Click **Next**.
10. At the Summary screen, click **Submit**.

6.1.4.2 Adding the Connection to the Database

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 BPEL server is named `WORKFLOW_CONNECTION`, and the `HelloBPEL` sample script uses the connection name `test`.

6.1.5 Configuring the GDFontPath MBean for a UNIX System

For conversions to work correctly on a UNIX operating system, it needs to have TrueType fonts available. If these fonts are not available on your system, you need to install them. To set the font path on a UNIX operating system, you need to configure the `GDFontpath` MBean. You can configure it through the System MBean Browser in Oracle Enterprise Manager Fusion Middleware Control.

To configure the GDFontPath MBean for a UNIX system:

1. Access the Imaging domain in Fusion Middleware Control at the following URL:

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

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

   ```
   http://myHost.example.com:7001/em
   ```

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

2. In the navigation tree on the left, expand **WebLogic Domain** and the deployed domain.
3. Right-click **IPM_server1**, and choose **System MBean Browser** from the menu.
4. In the navigation tree on the System MBean Browser page, under **Configuration MBeans**, close the **com.bea** folder.
5. Under **Application Defined MBeans**, expand the **oracle.imaging** folder.
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`
   - AIX: `/usr/lpp/X11/lib/X11/fonts/TrueType`
   - HP-UX Itanium: `/usr/lib/X11/fonts/TrueType`
   - Linux: `/usr/lib/X11/fonts/TrueType`

9. Click **Apply**.
10. Restart Imaging, as described in Section 10.3, "Restarting a Managed Server."

6.1.6 Setting DISPLAY for the Imaging Viewer in a UNIX Exalogic Environment with Solaris 11g

In an Exalogic environment with Solaris 11*g*, you need to set the DISPLAY environment variable for the Imaging Viewer to work correctly in basic mode.

To set DISPLAY for the Imaging Viewer in a UNIX Exalogic Environment with Solaris 11g:

1. Open a new terminal window and run this command:

   ```
   xhost +
   ```

2. In the Imaging terminal, set the DISPLAY environment variable to the server where Imaging is running and the port, in this format:

   ```
   servername:port
   ```

3. Restart Imaging, as described in Section 10.3, "Restarting a Managed Server."

6.1.7 Importing Definitions

At this point in the installation process, you can import previously exported Imaging definitions (applications, searches, and inputs). For more information, see "Exporting and Importing Definitions" in *Administering Oracle WebCenter Content: Imaging*.

For additional information about how to import definitions, see Section 6.5.1.2.2, "Importing Definition Files into Imaging."

6.2 Configuring the Full-Text Features in the WebCenter Content Repository

Imaging supports two types of full-text searching under WebCenter Content: `DATABASE.FULLTEXT` and `OracleTextSearch`. Imaging can use the full-text features if you configure full-text searching in the WebCenter Content repository first. For `DATABASE.FULLTEXT` systems, after the indexes are rebuilt, nothing needs to be done on the Imaging side. `OracleTextSearch`, however, requires that the index be rebuilt any time an application with `FullText` enabled is created, deleted, or has modifications that involve field definitions.

For more information on configuring full-text searching, see Section 4.5, "Configuring OracleTextSearch for Content Server."

For additional full-text configuration options, see "Configuring the Search Index" in *Administering Oracle WebCenter Content*.

After full-text is enabled in WebCenter Content, you will need to create an application and check the `FullText` option on the application. For more information, see "Configuring System Properties" in *Administering Oracle WebCenter Content*.

6.3 Setting Imaging System Security

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

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

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

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

   For more information, see Section 3.9, "Reassociating the Identity Store with an External LDAP Authentication Provider."

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

   For more information, see the *WebLogic Scripting Tool Command Reference*.

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

6.4 Configuring the Imaging Viewer Cache

The Imaging viewer can cache documents on the server outside of the repository to increase rendering speed on the client machine. Security for the cached documents is controlled by authentication for the server on which they are stored. If the server is considered secure, no additional security is necessary. If additional security is required, cached documents can be encrypted, as described in Section 6.4.2, "Encrypting Cached Documents."

To set the Imaging viewer to use cached documents:

1. Verify that the Imaging Viewer Cache was successfully deployed:

   a. In the WebLogic Server Administration Console, click **Deployments** under Domain Structure on the left,

   b. In the `imaging-vc` row of the **Deployments** table, confirm that the **State** value is `Active` and the **Health** value is `OK`.

   If the **State** or **Health** value is different for `imaging-vc`, you need to fix the deployment or redeploy the feature before proceeding.

2. Enable viewer caching by setting the **ViewerCachePath** MBean to the location where documents should be cached, using the method described in Section 6.1.5, "Configuring the GDFontPath MBean for a UNIX System." For example, to enable caching on an Imaging system running on a single computer, the relative path `imaging/ViewerCache` can be used. If no path is set, then caching of documents is disabled.

> **Note:** The **ViewerCachePath** MBean should be set to a location available to all servers in the cluster. If the directory path is not available to all servers, then each server will cache documents locally, resulting in multiple instances of the entire cache.

3. Specify the number of days for documents to remain in the cache location after being viewed by setting the **ViewerCacheDays** MBean. Cached documents not viewed within the specified number of days are purged from the cache. If a document is viewed within the specified number of days, the **ViewerCacheDays** timer for that document is reset. Setting **ViewerCacheDays** equal to `0` (the default) prevents the cache from being purged.
4. Set the **ViewerCacheEnablePrecache** MBean to `true` to cache documents when they are ingested into Imaging (precache) or to `false` to cache documents when they are first called by the viewer.

6.4.1 Changing the Viewer Cache Path

You can move the viewer cache to a new location provided the Imaging server is shut down and the new location uses the same file hierarchy as the old location.

1. Shut down the Imaging server.
2. Move the cached files to the new location, preserving the file hierarchy.
3. Set the new path in the **ViewerCachePath** MBean.
4. Start the Imaging server.

6.4.2 Encrypting Cached Documents

If additional security is required, Imaging can be configured to encrypt cached documents. Encryption makes additional processing necessary to decrypt a document for viewing and reduces rendering speed. Even if Imaging is configured to encrypt the cached documents, there is a brief period of time during caching when generated documents are not encrypted.

To enable encryption of cached documents:

1. Add a new password credential to the domain with Oracle Enterprise Manager Fusion Middleware Control:
   a. Select the WebLogic Server domain for Oracle WebCenter Content.
   b. From the **WebLogic Domain** menu, select **Security** and then **Credentials**.
   c. Select the map **oracle.imaging**. If no map named `oracle.imaging` exists, click **Create Map**, enter **oracle.imaging** for the map name, and then select it.
   d. Click **Create Key**. Name the key **viewer.cache**, and select the type **Password**.
   e. Enter a user name. The user name does not need to exist in any system.
   f. Enter a password, confirm it, and then click **OK**.
2. Enable encryption by setting the **ViewerCacheEnableEncryption** MBean, using the method described in Section 6.1.5, "Configuring the GDFontPath MBean for a UNIX System."

> **Note:** The password credential must exist on the domain before you set the **ViewerCacheEnableEncryption** MBean.

6.4.3 Disabling Encryption of Cached Documents

Encryption of cached documents can be disabled by setting the **ViewerCacheEnableEncryption** MBean to `false`. Subsequent calls to the viewer will cause unencrypted documents to be cached. Any encrypted documents still in the cache can be decrypted and viewed provided the password credential remains in the domain unaltered.

Purging the imaging.jks File If the Password Credential Is Removed or Altered

If the password credential is removed or altered, encrypted documents still cached must be manually purged.

To purge the `imaging.jks` file:

1. Shut down the Imaging server.
2. Delete the cached files from the cache directory.
3. Delete the `imaging.jks` file from the cache directory.
4. Start the Imaging server.

6.5 Installing and Configuring AXF for BPM and AXF for BPEL

Oracle WebCenter Content: AXF for BPM and Oracle Application Extensions Framework (AXF) for BPEL are installed automatically with Imaging, and AXF for BPEL is automatically deployed to the Imaging Managed Server. Before you can deploy AXF for BPM to the Imaging server, you need to create the required schemas with the Repository Creation Utility, as described in Section 2.2.2, "Creating Schemas for Oracle WebCenter Content Applications." Then when the domain is created or extended, you can select AXF for BPM to use it with Imaging, as described in Chapter 3, "Configuring Oracle WebCenter Content Applications."

You can configure either AXF for BPM or AXF for BPEL, or both, to run on the Imaging Managed Server:

- AXF for BPM

  The newer AXF for BPM infrastructure takes advantage of the application development and configuration capabilities provided by technologies such as Oracle Business Process Management (Oracle BPM), Oracle Application Development Framework (Oracle ADF), Oracle Metadata Services Repository (Oracle MDS Repository), and Oracle Business Rules to create configurable business components. Administrators can use these business components to configure and develop integration solutions for WebCenter Content business applications.

  For more information, see Section 6.5.1, "Configuring and Verifying AXF for BPM."

- AXF for BPEL

  The older AXF for BPEL infrastructure relies on AXF database tables (Imaging tables) as the basis for configuring AXF solutions, commands, and web tools. A solution developer or solution accelerator can implement and customize these solutions, commands, and tools.

  For more information, see Section 6.5.2, "Configuring and Verifying AXF for BPEL."

For additional information about configuring and using AXF for BPM or AXF for BPEL and the AXF for BPEL database tables (Imaging tables), see *Administering the Application Adapters for Oracle WebCenter*.

6.5.1 Configuring and Verifying AXF for BPM

Before you configure AXF for BPM with Imaging, you need to install and configure 11*g*R1 (11.1.1.9.0) Oracle WebCenter Content and Oracle SOA Suite and create an AXF schema with the Repository Creation Utility as well as schemas for the following components:

- **Metadata Services**
- **Oracle WebCenter Content Server - Complete**
- **Oracle WebCenter Content: Imaging**
- **SOA Infrastructure**
- **User Messaging Service**

When you create or extend the WebLogic Server domain, be sure the following product templates are selected:

- **Oracle SOA Suite**
- **Oracle WebCenter Content: AXF for BPM**

> **Note:** If AXF for BPM is on a separate host machine from the Oracle SOA Suite Managed Server, the domain will need to be extended with Oracle WSM Policy Manager.

- **Oracle WebCenter Content: Imaging**
- **Oracle Universal Content Management - Content Server**

  (for WebCenter Content)
- **Oracle Enterprise Manager**
- **Oracle BPM Suite**

After you create or extend a domain to include AXF for BPM and the components and products it depends on, you can configure it to work with Imaging using the WebLogic Server Administration Console, Oracle WebLogic Server Scripting Tool (WLST), and Oracle Enterprise Manager Fusion Middleware Control. Section 6.5.1.1, "Configuring AXF for BPM," describes how to do this. It also describes how to set up communications with Oracle Coherence between AXF for BPM and Imaging servers running on multiple domains or machines or to prevent multicast interference between AXF for BPM and Imaging in a single domain.

For verification that the AXF for BPM infrastructure is properly installed and configured, AXF for BPM includes the `HelloBPM` solution, which uses an Oracle BPM process to verify the BPM integration. Section 6.5.1.2, "Verifying the AXF for BPM Installation," describes how to deploy and use this solution.

6.5.1.1 Configuring AXF for BPM

Use the following procedure to configure AXF for BPM with the Imaging server. You can set up the Imaging server through the WebLogic Server Administration Console, create foreign JNDI with WLST, and configure the AXF for BPM CSF key through Fusion Middleware Control.

To configure AXF for BPM to work with Imaging Managed Servers that run in a cluster or other distributed configuration, you need to set up communications with Oracle Coherence, as Section 6.5.1.1.1, "Oracle Coherence Communications for Imaging Clusters, Multiple Domains, or Multiple Machines," describes. In a single domain, you can set up communications with Oracle Coherence to avoid interference from multicast traffic, as Section 6.5.1.1.2, "Oracle Coherence Communications for a Single Server or Domain," describes.

To configure AXF for BPM:

1. Set up the Imaging server through the WebLogic Server Administration Console:

   a. The Administration Server should already be running. If not, 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 Administration Console.

   c. Under **Domain Structure** on the left, expand **Environment**, and click **Servers**.

   d. In the **Servers** table, click the Imaging server instance, such as **IPM_server1**.

   e. Click the **Protocols** tab.

      If the server is in production mode, you need to click the **Lock & Edit** button in the Change Center on the left before you can make changes on this tab.

   f. Click the **HTTP** subtab.

   g. Set these values:

      * **Frontend Host**: The name of the host machine for the Imaging server, such as `myserver.example.com`

      * **Frontend HTTP Port**: The port number for the Imaging instance, such as `16000`

   h. Save the changes.

      If the server is in production mode, you need to activate changes after you save them, unless configuration editing is enabled.

2. If the Oracle SOA Suite Managed Server is on a separate host machine from Imaging, set the targeting for the `IPMDS` and `mds-axf` data sources to the Oracle SOA Suite server:

   a. Log in to the Administration Console on the Oracle SOA Suite machine.

   b. Under **Domain Structure** on the left, expand **Services**, and click **Data Sources**.

   c. Choose **Generic Data Source** from the **New** menu.

   d. Enter `jdbc/IPMDS` in the **JNDI Name** field.

   e. Select your database type in the **Database Type** list, and click **Next**.

   f. Configure values for **Data Source Properties** to match the connection of the same name on the corresponding Imaging server, including using the same schema.

   g. Test the configuration to ensure everything is valid.
   h. Click **Finish**.
   i. On the **Configuration** tab of the Summary of JDBC Data Sources page, click **IPMDS**.
   j. Click the **Targets** tab.
   k. Select the name of the Oracle SOA Suite server.
   l. Click **Save**.
   m. Return to the **Configuration** tab on the Summary of JDBC Data Sources page, and click **mds-axf**.
   n. Click the **Targets** tab.
   o. Select the name of the Oracle SOA Suite server.
   p. Click **Save**.

3. If the Oracle SOA Suite Managed Server is on a separate host machine from Imaging, create a `SOALocalTxDataSource` data source on the Imaging server as it is set up on the Oracle SOA Suite server:
   a. Log in to the Administration Console on the Imaging machine.
   b. Under **Domain Structure** on the left, expand **Services**, and click **Data Sources**.
   c. On the **Configuration** tab of the Summary of JDBC Data Sources page, choose **Generic Data Source** from the **New** menu.
   d. Enter `SOALocalTxDataSource` in the **Name** field.
   e. Enter `jdbc/SOALocalTxDataSource` in the **JNDI Name** field.
   f. Select your database type in the **Database Type** list, and click **Next**.
   g. Configure values for **Data Source Properties** to match the connection of the same name on the corresponding Oracle SOA Suite server, including using the same schema.
   h. Test the configuration to ensure everything is valid.
   i. Click **Next** to select targets.
   j. Select the name of the Imaging server.
   k. Click **Finish**.

4. Create foreign JNDI with the Oracle WebLogic Scripting Tool (WLST):
   a. Change to the `*WCC_ORACLE_HOME*/axf_bpm/scripts` directory.
   b. Edit the `create-foreign-JNDI.py` script using a text editor.

c. Set the following variables at the top of the file:

```
# host to login to for executing script
var_host = "" # (-h) WebLogic Server Administration Server host name
var_hostPort = "" # (-p) Administration Server port
var_user = "" # (-u) WebLogic Server User Name
var_credential = "" # (-c) WebLogic Server Password
# JNDI settings
var_jndiURIServer = "" # (-t) JNDI target URI of Oracle SOA Suite host
var_jndiURIServerPort = "" # (-v) JNDI target URI port
var_serverTargetName = "" # (-s) Managed Server name, for targeting the
Imaging server
var_jndiUser = "" # (-n) JNDI user name
var_jndiPassword = "" # (-d) JNDI password
```

d. Save the file.

e. Run the `create-foreign-JNDI.py` script against the Imaging server with WLST.

The WebLogic Server should be the only server running when you execute the script, as follows:

```
cd WCC_ORACLE_HOME/common/bin
./wlst.sh create-foreign-JNDI.py
```

5. Configure the AXF for BPM CSF key:

a. Log in to Oracle Enterprise Manager Fusion Middleware Control.

b. Navigate to the WebLogic Server domain and right-click the deployed domain (`base_domain` by default).

c. In the resulting menu, choose **Security** and then **Credentials**.

d. Create a new map:

Specify the map name, `oracle.wsm.security`.

e. Create a new key:

* Specify a key name, such as `ipmadmin`.

* Specify a valid administrator user, such as `weblogic`.

* Specify the password.

* After you specify the key name, user, and password, click **OK**.

6.5.1.1.1 Oracle Coherence Communications for Imaging Clusters, Multiple Domains, or Multiple Machines If you are configuring AXF for BPM, you should configure communications with Oracle Coherence, which AXF for BPM utilizes. By default the server is set up for clustering with the following settings configured in the *`DOMAIN_HOME`*`/bin/setDomainEnv.sh` script:

```
-Dtangosol.coherence.clusteraddress=224.3.1.99
-Dtangosol.coherence.clusterport=3199
-Dtangosol.coherence.log=jdk
```

In an Imaging cluster, you need to set up AXF for BPM communications with Oracle Coherence with a unique multicast address and port to avoid unwanted multicast traffic from interfering with the system. For more information about configuring Oracle Coherence in clusters, see the *Oracle Coherence Developer's Guide*.

6.5.1.1.2 Oracle Coherence Communications for a Single Server or Domain

For a single-server or domain installation, you can configure Oracle Coherence to avoid the multicast traffic of other machines by editing the *DOMAIN_HOME*/bin/setDomainEnv.sh script as follows:

1. Open the *DOMAIN_HOME*/bin/setDomainEnv.sh script in a text editor.
2. Perform a search for "coherence" to locate any existing settings.
3. Append the following two setting after any existing Oracle Coherence settings; for instance, after -Dtangosol.coherence.log=jdk:

   ```
   -Dtangosol.coherence.localhost=127.0.0.1
   -Dtangosol.coherence.ttl=0
   ```

4. Save the settings.
5. Restart any running Managed Servers on the domain for the changes to take effect.

6.5.1.2 Verifying the AXF for BPM Installation

You can verify the AXF for BPM installation and configuration with the HelloBPM solution, which uses a BPM process. The following sections describe how to deploy and use this solution:

- Section 6.5.1.2.1, "Configuring the HelloBPM Solution"
- Section 6.5.1.2.2, "Importing Definition Files into Imaging"
- Section 6.5.1.2.3, "Accessing the Solution Administration Page"
- Section 6.5.1.2.4, "Injecting Tasks into Imaging"

6.5.1.2.1 Configuring the HelloBPM Solution

Before you can use the HelloBPM solution to validate the installation and configuration of AXF for BPM, you need to deploy and configure the solution on the Imaging Managed Server.

To configure the HelloBPM solution:

1. Set up the database:

   a. Change to the *WCC_ORACLE_HOME*/axf_bpm/scripts directory.

   b. Run the AXF_HELLO_BPM_DATA.sql script while connected to the Imaging database schema as the Imaging database user, with the following three parameters:

      * *SOAMachineName*:*Port*
      * *IPMMachineName*:*Port*
      * *CSFKEY*

      This will insert the data necessary to run the HelloBPM solution.

2. If the Oracle SOA Suite Managed Server is on a separate host machine from Imaging, the Hello BPM process will need to be manually deployed.

   Copy the *WCC_ORACLE_HOME*/axf_bpm/bpm/sca_axfHelloBPM_rev1.0.jar file to DOMAIN_HOME/soa/autodeploy/ prior to starting the Oracle SOA Suite Managed Server.

3. Start up the remaining servers in the following order. For more information about starting the servers, see Section 10.2, "Starting Managed Servers," and Section 10.4,

"Using Node Manager with Oracle WebCenter Content."

   a. Weblogic Server Administration Server (should already be running)
   b. Oracle SOA Suite Managed Server
   c. Imaging Managed Server
   d. WebCenter Content Managed Server

4. Verify that a URI is set on the deployed process:
   a. Log in to Oracle Enterprise Manager Fusion Middleware Control.
   b. Navigate to the Oracle SOA Suite Managed Server, then `soa-infra (soa_server1)`, and then `default`, and click `axfHelloBPM`.
   c. In the Component Metrics section, click `SalesQuoteEntry`.
   d. Click the **Administration** tab.
   e. If a valid URI is not set, create one with these settings:
      * **Application Name**: `worklist`
      * **Host Name**: The name of the host machine for the server
      * **HTTP Port**: The port of the host machine for the server
      * **HTTPS Port**: The secure port of the host machine for the server, or the default value if SSL is not configured
      * **URI**: `/workflow/axfSolutionHelloBPM/faces/adf.task-flow?_id=SalesQuoteEntry_TaskFlow&_document=WEB-INF/SalesQuoteEntry_TaskFlow.xml`

6.5.1.2.2 Importing Definition Files into Imaging

You can import definition files for tasks into the Imaging server through the Imaging Injector.

To import definition files into Imaging:

1. Create the connections:
   a. Log in to Imaging as an administrator user, such as `ipmadmin`.

   > **Note:** This first user to connect to the Imaging system is registered as the Imaging administrator. For more information, see Section 6.1, "Completing the Initial Imaging Configuration."

   b. In the navigation tree on the left, expand **Manage Connections**.
   c. Choose **Create Content Server Connection** from the drop-down menu, and configure the connection:
      * On the Create Connection: Basic Information page, specify a name for the connection, and click **Next**.
      * On the Create Connection: Content Server Settings page, specify whether to use SSL, then specify whether to use a local Content Server (default) or specify an external server through the Content Server Pool section, and then click **Next**.
      * On the Create Connection: Security page, add the `Administrators` group with full rights, and click **Next**.

- Review your settings, and click **Submit**.

d. Choose **Create Workflow Connection** from the drop-down menu, and configure the connection:

- On the Create Connection: Basic Information page, specify a name for the connection, and click **Next**.
- On the Create Connection: Workflow Settings page, specify the following information, and then click **Next**.

  HTTP Front End Address: Specify the fully qualified HTTP address for the Oracle SOA Suite server:

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

  Credential Alias This should be the CSF key name specified in Section 6.5.1, "Configuring and Verifying AXF for BPM,", Step 5, such as `ipmadmin`.

  Provider: Specify the fully qualified `t3` address for the Oracle SOA Suite Server:

  ```
  t3://managedServerHost:managedServerPort/
  ```

- On the Create Connection: Security page, add the `Administrators` group with full rights, and click Next.
- Review your settings, and click **Submit**.

2. Import the definition file, *`WCC_ORACLE_HOME`*`/axf_bpm/ipm` into Imaging, using the definition import tool.

   For more information on uploading definitions and resolving environment configurations, including the repository connection and BPEL server connection as well as the security configurations of the applications, see *Administering Oracle WebCenter Content: Imaging*.

   a. In the navigation tree on the left, expand **Tools**.

   b. Choose **Import Definitions**.

   c. Browse to and select the *`WCC_ORACLE_HOME`*`/axf_bpm/ipm/HelloBPM.xml` file.

   d. Click **Next**.

   e. On the Select Definitions step, select the **Action** for **HelloBPM Application**, **HelloBPM Input**, and **HelloBPM Search**.

   f. Click **Next**.

   g. On the Validation step, select **Choose New** for the **Application Security** field, and select the **Administrators** group. Also choose the **Administrators** group for the **Applications, Document Security** field, **Inputs Security** field, and **Searches Security** field.

   h. For the **Workflow** field, select **Workflow Connection**.

   i. Click **Submit**.

6.5.1.2.3 Accessing the Solution Administration Page Before you can access the Solution Administration page, you need to set up an `axfadmin` group in WebLogic Server and assign your WebLogic Server user name to this group. For information about creating a group and adding a user to a group, see "Manage users and groups" in the WebLogic Server Administration Console Online Help.

To access administration functions for the solution application:

1. Open the new driver page:

   `http://*machinename*:16000/axf/faces/pages/axfadmin.jspx`

2. Click the **Command Driver** link, on the left.
3. Use the following values:
   a. **solutionNamespace**: `SalesQuoteEntry`
   b. **commandNamespace**: `StartSalesQuoteEntry`
4. Click the **Execute Request** button.
5. Click the **Execute Response** button.

The Solution Administration page opens. Table 6–1 shows the example parameters for this page.

Table 6–1 Parameters for the Solution Administration Page

Parameter	Value
`solutionNamespace`	`SalesQuoteEntry`
`commandNamespace`	`StartSalesQuoteEntry`
`Username`	The user name for the request

You can access the Business Rule Editor through the Solution Administration page and use this editor to perform any customizations. For more information, see *Administering the Application Adapters for Oracle WebCenter*.

6.5.1.2.4 Injecting Tasks into Imaging After you deploy the AXF for BPM process, you can inject tasks into Imaging either from the content input files, through the Imaging input agent, or from the Oracle SOA Suite server, through Oracle Enterprise Manager Fusion Middleware Control.

You can inject tasks into the `HelloBPM` solution from content input files that are installed with the AXF for BPM infrastructure. Injecting tasks through the Imaging input agent enables you to test solution application changes. If needed, you can modify the input files to match the `HelloBPM` workflows.

These content input files are in the following directory with *`WCC_ORACLE_HOME`*`/axf_bpm/ipm/HelloBPM.xml`, the Imaging application definition:

```
$WCC_ORACLE_HOME/axf_bpm/ipm/
```

This directory includes three input files:

- `TestSalesQuote.pdf`
- `TestSalesQuote.txt`
- `TestSalesQuote.xml`

The following procedure is based on the assumption that `InputDirectory` is left with the default configuration (`/IPM/InputAgent/Input`).

To inject tasks through the input agent:

1. Copy the PDF and XML files into the *`DOMAIN_HOME`* directory, and copy the TXT file into the *`DOMAIN_HOME`*`/IPM/InputAgent/Input` directory (default configuration).

You also might need to change file permissions so that `InputAgent` has access to these files.

For more information, see "Enabling Input Agent" in *Administering Oracle WebCenter Content: Imaging*.

Within the specified time interval (15 minutes by default), the input agent picks up the input files and creates a document with metadata values from the text input file, an image from the PDF file, and supporting content from the XML file.

Based on the workflow configuration in place with the `HelloBPM` solution, a task is created for the document that displays in the BPM task list.

2. In the task list, click the newly injected task to view its details in the solution application.
3. As needed, modify the metadata values in the text input file before injecting the input files again. For example, you might inject a task with missing account information to work with its human task flow.

6.5.2 Configuring and Verifying AXF for BPEL

To configure AXF for BPEL to work with Imaging Managed Servers that run in a cluster or other distributed configuration, you need to configure the Java Object Cache (JOC) to be distributed to all of the Managed Servers. For more information, see Section 6.5.2.1, "Configuring the Java Object Cache for AXF for BPEL in Distributed Imaging Managed Servers."

For verification that the AXF for BPEL infrastructure is properly installed, AXF for BPEL includes two simple solutions:

- `HelloWorld`, a basic solution that returns a `Hello` string

  See Section 6.5.2.2, "Verifying the AXF for BPEL Installation and Configuration with HelloWorld."

- `HelloBpel`, a solution that includes a BPEL process to verify the BPEL integration

  See Section 6.5.2.3, "Verifying the AXF for BPEL Installation and Configuration with HelloBpel."

6.5.2.1 Configuring the Java Object Cache for AXF for BPEL in Distributed Imaging Managed Servers

For AXF for BPEL in Imaging Managed Servers that run in a cluster, you need to configure a Java Object Cache (JOC) to be distributed to all of the Managed Servers. You can use HA Power Tools from the Oracle WebLogic Server Administration Console to configure the JOC for all of the Imaging Managed Servers that run in distributed mode.

> **Note:** After configuring the Java Object Cache, restart all affected Managed Servers for the configurations to take effect. For more information, see Section 10.3, "Restarting a Managed Server."

In the following instructions, *`MW_HOME`* represents the path to a Middleware home, where Oracle Fusion Middleware is installed, and *`DomainHome`* represents the path to the Oracle home for an Oracle WebLogic Server domain.

To configure the Java Object Cache for a cluster of distributed Managed Servers:

1. Enable HA Power Tools in the Oracle WebLogic Server Administration Console:

   a. Copy the following two WAR files from the *MW_HOME*/oracle_common/hapowertools directory to the *DomainHome*/console-ext directory:

      * powertools-core.war

      * powertools-configurejoc.war

      For example:

      ```
      cd middlewarehome
      cp oracle_common/hapowertools/powertools-co* user_projects/domains/base_
      domain/console-ext/
      ```

   b. Restart the Oracle WebLogic Server Administration Server.

      For more information, see Section 10.1, "Starting the Administration Server," and Section 10.3, "Restarting a Managed Server."

   c. Access the Oracle WebLogic Server Administration Console (at http://*adminServerHost*:*adminServerPort*/console), and click the name of your domain in the left navigation tree.

      The **HA Power Tools** tab appears on the Settings page for the domain.

2. Configure the distributed cache:

   a. On the Settings page for your domain in the Administration Console, click the **HA Power Tools** tab.

   b. On the **Configure JOC** tab, select **Configure JOC for Clusters**.

   c. In the **Cluster Name** field, choose a cluster name from the list.

   d. In the **Discover Port** field, enter the listener port number for the cluster.

   e. In the **Hosts** field, enter the names of all the Managed Server hosts, separated by commas.

   f. Click the **Configure JOC** button.

3. Restart the cluster of Managed Servers.

4. Verify the JOC distributed cache mode:

   a. From the Middleware home on the host for one of the Managed Servers, run the CacheWatcher utility, as in the following example:

      ```
      java -classpath oracle_common/modules/oracle.javacache_
      11.1.1/cache.jar:oracle_common/modules/oracle.odl_11.1.1/ojdl.jar
      oracle.ias.cache.CacheUtil watch -config=user_projects/domains/base_
      domain/config/fmwconfig/servers/IPM_server2/javacache.xml
      ```

      In this example, the class paths for the two JAR files are relative to the current directory (*MW_HOME*).

      The javacache.xml file is the file used by one of the Imaging servers that is participating in the JOC distributed cache. For a distributed Java cache with either virtual or physical IP addresses, the listener address needs to be set in javacache.xml. Each of the files should contain all the distributor location entries but only one <listener-address> entry, set to the same port number for every cache member, as follows:

      ```
      <listener-address port="portNumber1" host="hostName1"/>
      ```

```
<distributor-location ssl="true" port="portNumber1" host="hostName1"/>
<distributor-location ssl="true" port="portNumber1" host="hostName2"/>
<distributor-location ssl="true" port="portNumber1" host="hostName3"/>
<distributor-location ssl="true" port="portNumber1" host="hostName4"/>
```

b. Enter the `lc` command to list the cache information:

```
INFO: JOC is initialized from oracle.ias.cache.CacheUtil.main, . . .
cache> lc
```

c. In the output from the `lc` command, check that the Distributor Table shows an entry for each member of the distributed cache.

d. Enter the `exit` command to stop the CacheWatcher utility.

For more information, see "Using HA Power Tools" and "Running CacheWatcher" in *High Availability Guide*.

6.5.2.2 Verifying the AXF for BPEL Installation and Configuration with HelloWorld

Follow these steps to enable the `HelloWorld` solution:

1. As user who owns the Imaging schema, run the `insertHelloCommand.sql` script from one of the following directories.

   - **UNIX path:**
     MW_HOME/*WCC_ORACLE_HOME*/axf/drivers/HelloWorld/dbscripts
   - **Windows path:**
     MW_HOME\WCC_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 for BPEL 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 for BPEL response should display with a populated **Conversation ID**. If the response is returned, the AXF for BPEL infrastructure is functioning correctly, and commands can be added and executed.

6.5.2.3 Verifying the AXF for BPEL Installation and Configuration with HelloBpel

The `HelloBpel` solution includes a BPEL process and a SQL script to set up the `HelloBPEL` solution namespace for use by that process. The BPEL process and database script are in the following directories.

- **UNIX path:**
  MW_HOME/*WCC_ORACLE_HOME*/axf/drivers/HelloBpel
- **Windows path:**
  MW_HOME\WCC_ORACLE_HOME\\axf\\drivers\\HelloBpel

To enable the HelloBpel solution:

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

   - **UNIX scripts:**

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

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

   - **Windows scripts:**

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

     MW_HOME\WCC_ORACLE_HOME\axf\drivers\HelloBpel\dbscripts
     \sqlserver-db2\insertHelloBPELData.sql
     ```

   If you are using Oracle Database, then run the script from the `oracle` directory.

   If you are using an IBM DB2 or Microsoft SQL Server database, 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 Imaging Manage Connections section:

     ```
     Insert into AXF_SOLUTION_ATTRIBUTES (SOLUTION_NAMESPACE,PARAMETER_
     KEY,PARAMETER_VALUE) values ('HelloBPEL','BPEL_CONNECTION','test');
     ```

2. Run the `insertHelloBPELData.sql` script.
3. With Oracle JDeveloper 11*g*, open `HelloBPEL.jws` from following directory:

   - **UNIX path:**
     MW_HOME/*WCC_ORACLE_HOME*/axf/drivers/HelloBpel/bpel
   - **Windows path:**
     MW_HOME\WCC_ORACLE_HOME\\axf\\drivers\\HelloBpel\\bpel

   Deploy the process to your BPEL server. For assistance with this task, consult the 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 JDeveloper before deployment.

4. Access the driver page of the AXF for BPEL web application using the following URL:

   ```
   http://host:port/imaging/faces/Driver.jspx
   ```

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

   - **Solution Namespace:** `HelloBPEL`
   - **Command Namespace:** `StartHelloBPEL`
   - **User Name:** A valid Imaging user; for example, `weblogic`

   The preceding Imaging user needs to be part of a group named California. If this group does not exist, then create it, and add the user to the group.

6. Click **Execute Command**.

   A response should be displayed in the response screen.

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

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

7 Completing the Oracle WebCenter Enterprise Capture Configuration

This chapter explains how to complete the initial configuration of Oracle WebCenter Enterprise Capture in an Oracle WebLogic Server domain.

This chapter includes the following sections:

- Section 7.1, "About Completing the Oracle WebCenter Enterprise Capture Configuration"
- Section 7.2, "Completing the Initial Configuration of Oracle WebCenter Enterprise Capture"
- Section 7.3, "Creating a Hash Partition to Improve Database Performance"

7.1 About Completing the Oracle WebCenter Enterprise Capture Configuration

The Capture System Administrator who performs the installation and initial configuration must have system administration permissions, including access to Oracle Enterprise Manager Fusion Middleware Control and Oracle WebLogic Server. Before anyone can use Oracle WebCenter Enterprise Capture, a system administrator must associate users from the LDAP credential store for the WebLogic Server domain with the Capture roles in Fusion Middleware Control.

The roles `CaptureWorkspaceManager`, `CaptureWorkspaceViewer`, and `CaptureUser` are automatically added to the default WebLogic Server policy store for the domain. The Capture System Administrator can use the file/XML-based policy store, an Oracle Internet Directory policy store, or an Oracle Database policy store and manage the policy store through Fusion Middleware Control.

For more information about using Oracle Internet Directory Section 3.9, "Reassociating the Identity Store with an External LDAP Authentication Provider."

Through Fusion Middleware Control, you can also configure system settings and loggers for Capture.

7.2 Completing the Initial Configuration of Oracle WebCenter Enterprise Capture

To complete the initial configuration of Capture in a WebLogic Server domain, the Capture System Administrator needs to do these tasks:

1. Start the Capture Managed Server.
2. Assign roles to Capture users in Fusion Middleware Control.
3. Modify system-level settings through MBeans.

7.2.1 Starting the Capture Managed Server

For information about how to start the Capture Managed Server, see Section 10.2, "Starting Managed Servers."

7.2.2 Assigning Roles to Capture Users

Before anyone can use Capture, the Capture System Administrator needs to assign users from the LDAP credential store to the Capture roles in the policy store. You can do this through the Application Roles page in Fusion Middleware Control.

For information about how to assign roles to Capture users, see "Assigning Capture Roles in Oracle Enterprise Manager" in *Oracle Fusion Middleware Administering Oracle WebCenter Enterprise Capture*.

7.2.3 Modifying System-Level Settings

You can modify system-level configuration settings for Capture, including system properties and SMTP settings for email, through Fusion Middleware Control. The settings on this page configure the Capture MBeans for the domain, which you can also modify with Oracle WebLogic Scripting Tool (WLST) commands.

For information about how to modify system-level settings on the System Configuration page in Fusion Middleware control, see "Modifying System Configuration Settings" in *Oracle Fusion Middleware Administering Oracle WebCenter Enterprise Capture*.

The following WLST commands also enable you to access or modify system-level settings:

- `listCaptureConfig`
- `getCaptureConfig`
- `setCaptureConfig`

These are online WLST commands that you can use while connected to the Administration Server for the domain. To connect, you need to run the `wlst.sh` script from the Oracle WebCenter Content home directory.

To modify a Capture system-level setting with a WLST command:

1. Start the Administration Server for your Oracle WebLogic Server domain, as described in Section 10.1, "Starting the Administration Server."
2. Log in to the Oracle WebLogic Server Administration Server.
3. Navigate to the Oracle WebCenter Content home directory: *`MW_HOME/WCC_ORACLE_HOME`*.

4. Invoke WLST:

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

5. At the WLST command prompt, log in, and then enter a custom Capture command:

   ```
   wls:/offline> connect()
   Please enter your username :weblogic
   Please enter your password : XXXXXXXXXXXXX
   Please enter your server URL [t3://localhost:7001]
    :t3://host_name:16401
   Connecting to t3://host_name:16401 with userid weblogic ...
   Successfully connected to Managed Server 'capture_server1' that belongs to
   domain
   'domainName'.

   wls:/domainName/serverConfig> setCaptureConfig('CaptureSystemID','CAPTURE_02')

   Attribute 'CaptureSystemID' changed to "CAPTURE_02'

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

For more information about these commands, see "Oracle WebCenter Enterprise Capture Custom WLST Commands" in *Oracle Fusion Middleware Domain Template Reference*.

7.3 Creating a Hash Partition to Improve Database Performance

You can use a hash partition of the `EBATCTITEMS` table to minimize the database wait event `enq: HW- contention`, which prevents the database from scaling. This event occurs when many threads are trying to update and add new BLOB items to ECBATCHTITEMS, as follows:

```
table   - "UPDATE ECBATCHITEMS SET ECITEMDATA=:1 WHERE ECITEMID=:2"
```

Creating a hash partition minimizes this contention because different items will be in eight different partitions.

To create a hash partition:

1. Get the definition of the table:

```
SELECT dbms_metadata.get_ddl('OBJECT TYPE','OBJECT NAME', OWNER') FROM DUAL;
```

2. Append partitioning syntax to the table definition. The following table definition creates a hash partition for the ECBATCHITEMS table:

```
SQL> create table "CAPCLIENT_CAPTURE"."ECBATCHITEMS2"
  2     (    "ECTENNANTID" VARCHAR2(36 CHAR),
        "ECITEMID" VARCHAR2(36) NOT NULL ENABLE,
  3    4          "ECORIGINALITEMID" VARCHAR2(36),
  5          "ECORIGINALITEMINDEX" NUMBER(10,0),
  6          "ECBARCODES" BLOB,
  7          "ECBARCODECOUNT" NUMBER(10,0),
  8          "ECSTATUS" VARCHAR2(255),
  9          "ECSOURCEFORMAT" VARCHAR2(255),
        "ECANNOTATION" VARCHAR2(255),
10   11          "ECFILELENGTH" NUMBER(19,0),
12          "ECDOCUMENTLINKCOUNT" NUMBER(10,0),
13          "ECPATCHCODE" NUMBER(10,0),
14          "ECENDORSEMENT" VARCHAR2(255),
15          "ECSOURCEFILENAME" VARCHAR2(255),
16          "ECBATCHID" NUMBER(19,0),
17          "ECLASTMODIFIED" NUMBER(19,0),
18          "ECITEMDATA" BLOB,
         PRIMARY KEY ("ECITEMID")) partition by hash(ECITEMID) partitions 8
;
```

8 Completing the Records Configuration

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

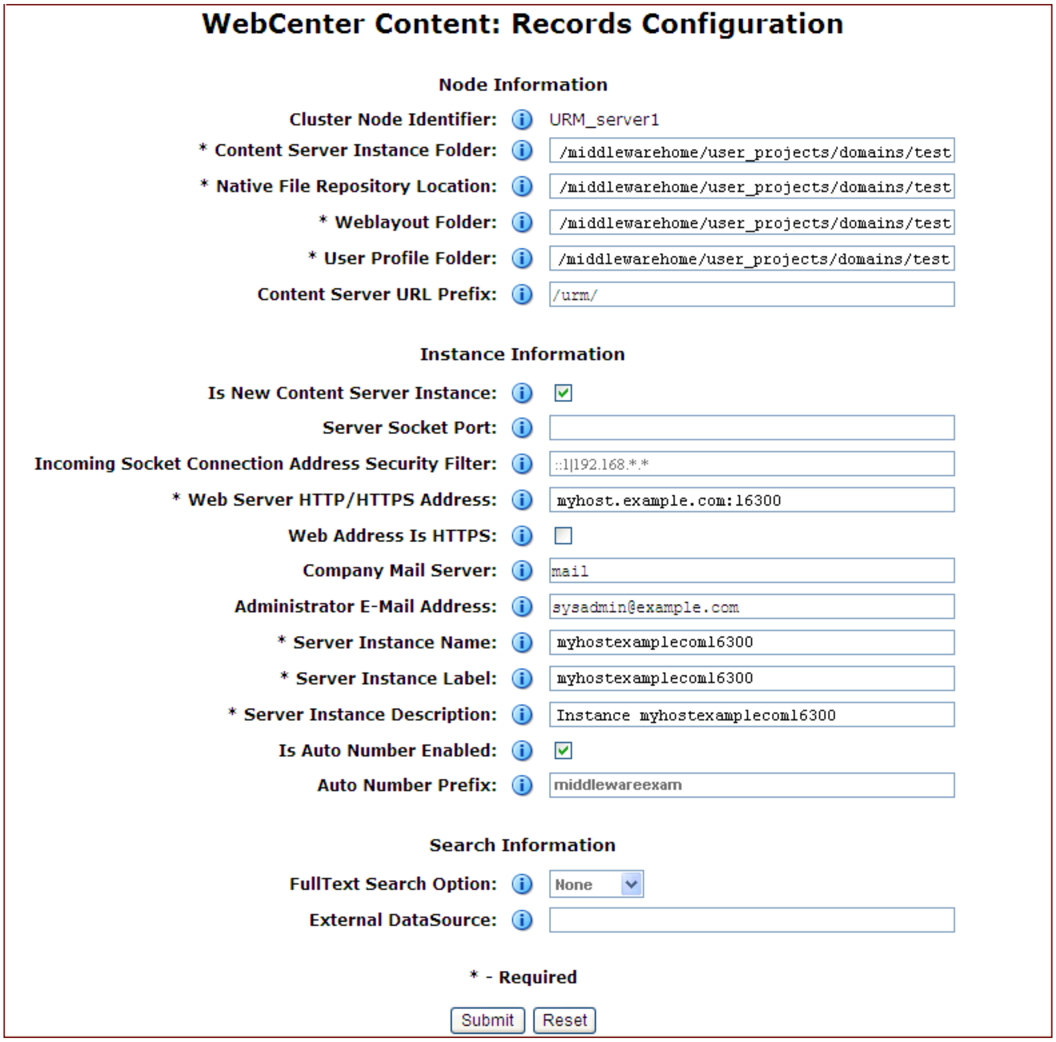
This chapter includes the following sections:

- Section 8.1, "Completing the Initial Records Configuration"
- Section 8.2, "Configuring Additional Parameters for Records Cluster Nodes"
- Section 8.3, "Using OracleTextSearch with Records"
- Section 8.4, "Setting Connection Pool Property Values for an IBM DB2 Data Source"

8.1 Completing the Initial Records Configuration

After installation and startup, when you go to the web interface for Records, you will get the WebCenter Content: Records Configuration page, which Figure 8–1 shows.

Figure 8–1 Configuration Page for Records



WebCenter Content: Records Configuration

Node Information

Cluster Node Identifier:	URM_server1
* Content Server Instance Folder:	/middlewarehome/user_projects/domains/test
* Native File Repository Location:	/middlewarehome/user_projects/domains/test
* Weblayout Folder:	/middlewarehome/user_projects/domains/test
* User Profile Folder:	/middlewarehome/user_projects/domains/test
Content Server URL Prefix:	/urm/

Instance Information

Is New Content Server Instance:	☑
Server Socket Port:	
Incoming Socket Connection Address Security Filter:	::1|192.168.*.*
* Web Server HTTP/HTTPS Address:	myhost.example.com:16300
Web Address Is HTTPS:	☐
Company Mail Server:	mail
Administrator E-Mail Address:	sysadmin@example.com
* Server Instance Name:	myhostexamplecom16300
* Server Instance Label:	myhostexamplecom16300
* Server Instance Description:	Instance myhostexamplecom16300
Is Auto Number Enabled:	☑
Auto Number Prefix:	middlewareexam

Search Information

FullText Search Option:	None
External DataSource:	

*** - Required**

For information about the fields on this page and the values you can enter to configure your Records instance, see Section 4.3.2, "Configuring the Content Server Instance." After you complete the WebCenter Content: Records Configuration page and click the **Submit** button, you need to restart Records, as described in Section 10.3, "Restarting a Managed Server."

When Records restarts, the web interface shows an alert:

```
Initial Records Management Setup is Not Complete!
```

Then you can select the Records install settings and installation level you want on the Configure: Enabled Features page and configure the features. For information about configuring these settings, see Section 8.1.1, "Configuring the Level of Records Features."

After you configure the installation level and features, you can complete the Records configuration through the Setup Checklist page. For more information, see Section 8.1.2, "Completing the Setup Checklist for Records."

Note: The `ContentFolios` component is required for access to the Records web interface. This component is enabled by default in a Records Managed Server. Do not disable the `ContentFolios` component.

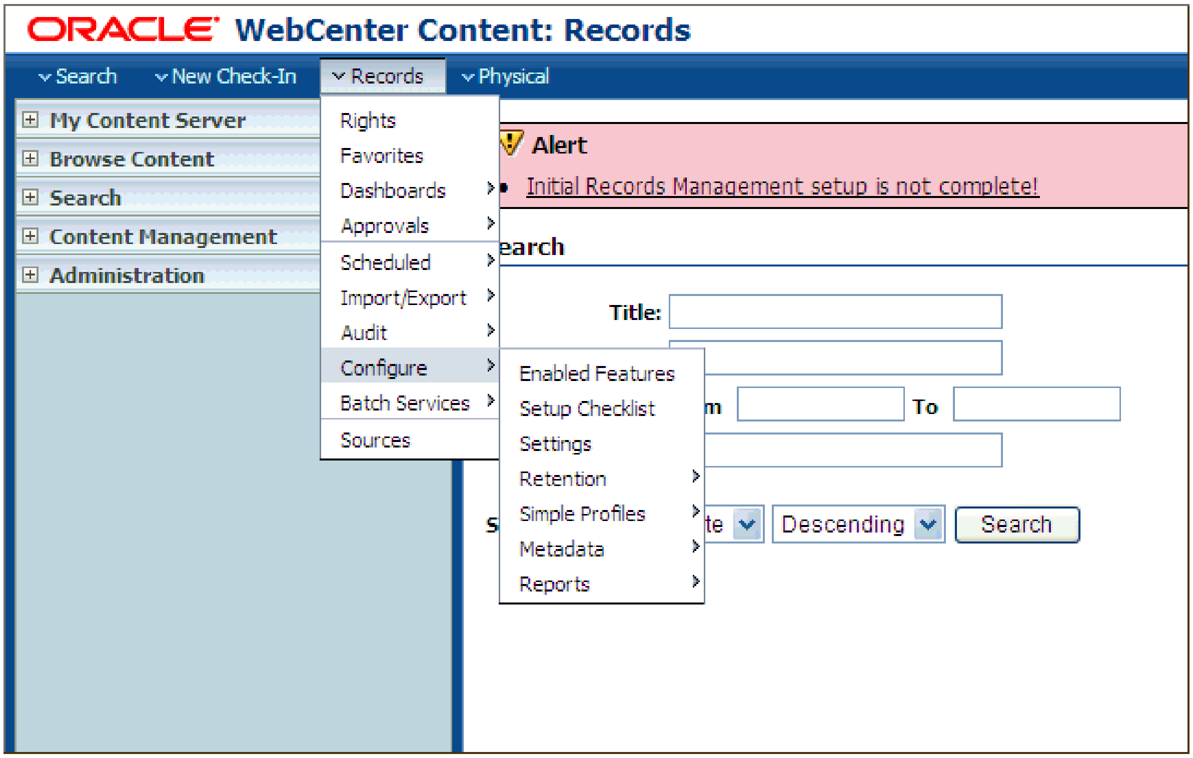
8.1.1 Configuring the Level of Records Features

On the Enabled Features page, you can configure and installation level and features for Records. The default installation level is **Minimal**.

To configure the level of Records features:

1. From the **Records** menu, choose **Configure**, then choose **Enabled Features**, as Figure 8–2 shows.

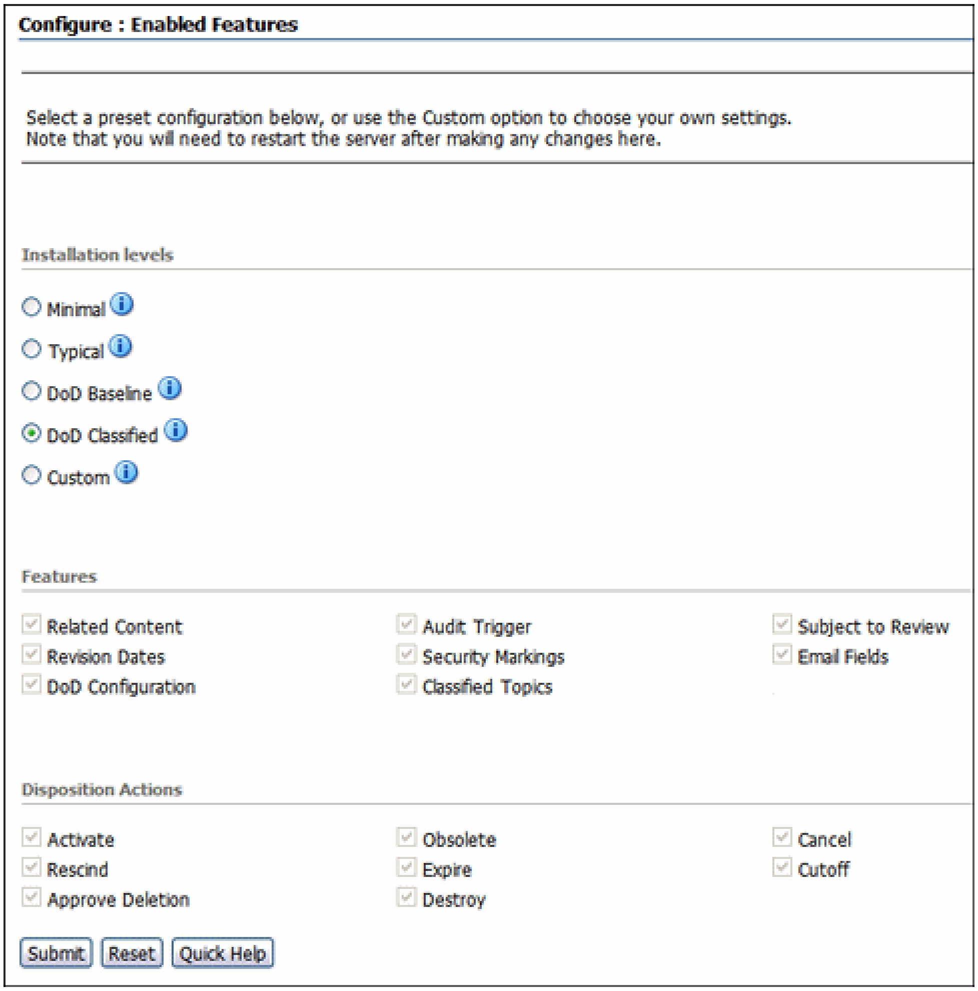
Figure 8–2 Records Menu



- Initial Records Management setup is not complete!

2. On the Enabled Features page, which Figure 8–3 shows, select an installation level, which selects all the features and disposition actions for that level.

Figure 8–3 Enabled Features Page



Configure : Enabled Features

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
○ Typical
○ DoD Baseline
● DoD Classified
○ Custom

Features

☑ Related Content
☑ Revision Dates
☑ DoD Configuration
☑ Audit Trigger
☑ Security Markings
☑ Classified Topics
☑ Subject to Review
☑ Email Fields

Disposition Actions

☑ Activate
☑ Rescind
☑ Approve Deletion
☑ Obsolete
☑ Expire
☑ Destroy
☑ Cancel
☑ Cutoff

The following table describes the installation levels and features that can be enabled. For information about the components to be enabled for each level, and the features and disposition actions to be installed, click the **Info** icon next to the level.

Element	Description
Installation Level	Specifies the type of configuration to be enabled: ■ Minimal ■ Typical ■ DoD Baseline ■ DoD Classified ■ Custom

Element	Description
Features	When you select an installation level, the default features for that level are selected to be enabled. If you select the **Custom** installation level, you can select the features you want enabled: ■ Related Content ■ Audit Trigger ■ Subject to Review ■ Revision Dates ■ Security Markings ■ Email Fields ■ DoD Configuration ■ Classified Topics
Disposition Actions	This section contains the disposition actions that can be used for content: ■ Activate ■ Rescind ■ Approve Deletion ■ Obsolete ■ Expire ■ Destroy ■ Cancel ■ Cutoff

---

Note: If you are using Oracle WebCenter with Records and want to use the DOD feature, you can set the DoD Baseline or Classified Installation level after WebCenterConfigure has been enabled and has had a chance to check in its conversion templates.

If you select a DOD installation level first, you can create a rule that matches the documents created by WebCenterConfigure to assign them to a default category. The category could be based on the content IDs. For more information, see "Setting Up Workflows" in *Managing Oracle WebCenter Content*.

---

3. If you selected the **Custom** installation level, select the features and disposition actions that you want enabled, and deselect any that you do not want enabled.
4. Click the **Submit** button.

After making selections or if configuration options are changed (for example, switching from **Baseline** to **Classified**), you need to restart the Records Managed Server and rebuild the Content Server index. For more information, see Section 8.1.2, "Completing the Setup Checklist for Records." For information about rebuilding the index, see "Working with the Search Index" in *Administering Oracle WebCenter Content*.

8.1.2 Completing the Setup Checklist for Records

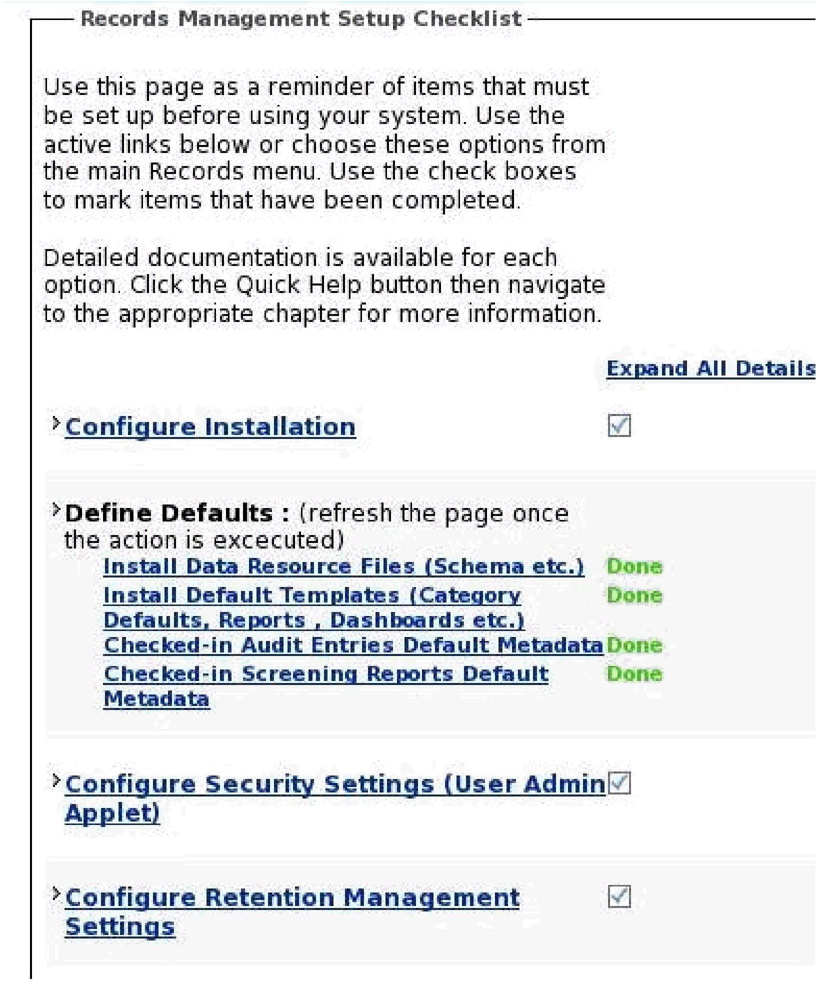
After the installation and configuration of Records on a Managed Server, you need to complete the Setup Checklist page before you can set up retention policies and procedures. This page is used to set global options for aspects of the retention management system.

For information about setting up retention policies and procedures, see "Retention Management Options" in *Managing Oracle WebCenter Content*.

To complete the Setup Checklist for Records:

1. From the **Records** menu, choose **Configure** then choose **Setup Checklist**.
2. On the Setup Checklist page, which Figure 8–4 shows, for each action that is marked **Not Done**, click the action, complete the configuration for it, refresh the Setup Checklist page, and then mark the checkbox to the right of the action to indicate that it is complete.

Figure 8–4 Records Setup Checklist



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 excecuted)

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

› Configure Security Settings (User Admin Applet) ☑

› Configure Retention Management Settings ☑

If any required configuration tasks on this page are not completed, a warning message with a link to this page appears on the home page of the Records system. You can click the link to display this page, or you can display the page from the **Records** menu again.

> **Note:** The Configure Report Library task is only for the Records Management feature in Content Server. This library is not needed for Oracle WebCenter Content: Records. For information about how to configure the report library, see Section 4.1, "Configuring the Report Library for Records Management in Content Server."

3. For any of the other actions that you want to configure, click the action, complete the configuration for it, refresh the Setup Checklist page, and then mark the checkbox to the right of the action to indicate that it is complete.

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

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

   The following table lists the actions that can be on the Setup Checklist and describes the purpose of each action.

Action	Description
Configure Installation	Used to configure optional components and metadata fields. Select from preset configurations to choose the features that are needed.
Configure Report Library	Used to configure the report library for the Records Management feature of Content Server, after adding the `oracle.xdo.runtime` library from the Oracle WebLogic Server Administration Console and a library reference to `weblogic-application.xml` This library is not needed for Oracle WebCenter Content: Records.
Define Defaults	Used to define the default for audit trails, template locations, and metadata for content that is automatically checked in on a periodic basis. You can configure metadata for Audit Entries and for Screening reports. Clicking an option brings up a check in page where you can edit the fields to be used as defaults.
Configure Security Settings	Used to define the security settings including roles, rights, and access control list use. This link opens the Admin Applets. Click the User Applet to configure security.
Configure Retention Management Settings	Used to configure many of the retention management options such as supplemental markings, triggers, and reports. Clicking this option displays the Configure Retention Settings page. For more information, see "Retention Management Options" in *Managing Oracle WebCenter Content*.
Configure Fiscal, Calendar, and Custom Periods	Used to set periods used for disposition processing. Selecting this option displays the Configure Periods page. For information, see "Managing Time Periods" in *Managing Oracle WebCenter Content*.

Action	Description
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, see "Working with Triggers" in *Managing Oracle WebCenter Content*.
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 *Managing Oracle WebCenter Content*.
Configure Freeze Reasons	Used to set up freezes. Selecting this option displays the Freeze Configuration page. For more information, see "Managing Freezes" in *Managing Oracle WebCenter Content*.
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 *Managing Oracle WebCenter Content*.
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 *Managing Oracle WebCenter Content*.
Configure Federated Search Default Category	Used to indicate a default category and default folder to use for Federated searches. Selecting this option displays the Component Manager page, where you can enter configuration variables: ■ `FederatedSearchDefaultCategory=categoryId` ■ `FederatedSearchDefaultFolder=folderId`
Configure 'Profile Trigger' as Trigger Field	Used to determine the trigger for profiles used in searching and checking in content and physical items.

There is no longer an installation requirement that the `NumConnections` configuration variable be set to `10`. This configuration is now controlled by Oracle WebLogic Server and does not need to be set independently.

8.2 Configuring Additional Parameters for Records Cluster Nodes

For Records cluster nodes, you need to add some additional parameters to avoid performance problems such as stuck threads or other file system issues.

Using a text editor, add the following options to each cluster node's *DOMAIN_HOME*/ucm/urm/bin/intradoc.cfg file, where the directories specified are on a direct-bus-attached-controlled *local* disk and not a remote file system, such as a Windows mapped drive to NTFS/CIFS, or a UNIX/Linux mounted NFS or clustered file system (like OCFS2, GFS2, or GPFS):

```
TraceDirectory=local_domain_home/servers/URM_serverN/logs/
EventDirectory=local_domain_home/servers/URM_serverN/logs/event/
ArchiverDoLocks=true
DisableSharedCacheChecking=true
```

For each cluster node created with the Oracle WebLogic Scripting Tool (WLST) unpack command, you will need to create the preceding directories, ensuring that the permissions are the same as for the first installed node (RWXD for the user executing the Records Managed Server, usually oracle). The trailing *N* should match the node's server name, like URM_server1 is node 1, URM_server2 is node 2, and so on.

Note: The directories can reside in any local disk path that you have determined to have enough space to hold the Records logs and any trace that you might configure. The preceding paths are suggestions.

Finally, add one more parameter, which must be on a *shared* file system (unlike the other entries, which should point to the local disk installation):

```
UserProfilesDir=ORACLE_BASE/admin/domain_name/urm_cluster_
name/urm/data/users/profiles/
```

Note: A Records Managed Server cannot be configured for server migration.

8.3 Using OracleTextSearch with Records

When you use OracleTextSearch with Content Server, 32 optimized fields are allowed. When Records is installed, the number of optimized fields can exceed the 32-field limit.

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

If you install Records while using OracleTextSearch and later change search engines, you can configure the date fields to be searchable by using the Content Server Configuration Manager.

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

To search auxiliary metadata in Records with Oracle Text 11*g*, you must configure Content Server to use `OracleTextSearch` as the search engine. You can set `OracleTextSearch` on the WebCenter Content postinstallation configuration page or in the configuration file. For more information, see Section 4.5, "Configuring OracleTextSearch for Content Server."

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

If the Records Managed Server has an IBM DB2 data source, you need to set the `DynamicSections` property value to at least `500` in the connection pool configuration for the data source. This setting can prevent a `DYNAMICSECTIONS` error.

To set connection pool property values for an IBM DB2 data source:

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

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

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

   ```
   http://myHost.example.com:7001/console
   ```

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

2. Click **Services** in the navigation tree on the left.
3. Click **JDBC** in the **Section** column under Summary of Services.
4. Click **Data Source** in the **Section** column under Summary of Services: JDBC.
5. Click **URDMS**, or the JNDI name of the data source for the Records Managed Server, in the Data Sources table.
6. On the Settings page for the data source, click the **Connection Pool** tab.
7. In the **Properties** field, add the following lines to the list of properties to be passed to the JDBC driver:

   ```
   createDefaultPackage=true
   replacePackage=true
   dynamicSections=500
   ```

8. Click the **Save** button.

9

Completing the Oracle IRM Configuration

This chapter explains how to complete the initial configuration of Oracle Information Rights Management (Oracle IRM) in an Oracle WebLogic Server domain.

This chapter includes the following sections:

- Section 9.1, "Completing the Initial Oracle IRM Configuration"
- Section 9.2, "Validating the Oracle IRM Configuration"
- Section 9.3, "Configuring the Identity Store"
- Section 9.4, "Integrating Rights with Oracle Access Manager 11g"
- Section 9.5, "Configuring Oracle IRM to Use Oracle RAC"

9.1 Completing the Initial Oracle IRM Configuration

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

- Setting the Server URL Configuration Parameter for Oracle IRM
- Configuring a Keystore for Oracle IRM

> **Note:** In a production environment, Oracle WebCenter Content applications need to use an external Lightweight Directory Application Protocol (LDAP) authentication provider rather than the Oracle WebLogic Server embedded LDAP server, which is part of the default configuration. If you want to reassociate the identity store for Oracle IRM with an external LDAP authentication provider, it is easier to do this before you complete the configuration of the Oracle IRM Managed Server. For more information, see Section 3.9, "Reassociating the Identity Store with an External LDAP Authentication Provider."

9.1.1 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 Oracle IRM Managed Server. For example:

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

To set the Server URL configuration parameter:

1. Start Fusion Middleware Control at the following website:

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

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

   ```
   http://myHost.example.com:7001/em
   ```

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

2. In the farm navigation tree on the left, expand **WebCenter Content** and **Rights**, and then click **IRM**.
3. From the **IRM** menu, select **Administration** and then **General Settings**.

   Fusion Middleware Control displays the General Settings page.

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

   For a simple installation where the Managed Server is directly accessible to Oracle IRM Desktop, this value will be the URL of the Oracle IRM Managed Server, ending in `irm_desktop`:

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

   The *`managedServerHost`* value is the name of the host where the Managed Server is running, such as `myhost.example.com`. The default SSL port for Oracle IRM (*`managedServerPort`* value) is `16101`.

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

5. Click **Apply**.

9.1.2 Configuring a Keystore 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 keystore before contexts can be created.

Access to the keystore requires a password, and access to the wrapping key requires an additional password. Both passwords are stored in the credential store.

To configure a keystore for Oracle IRM, you need to do the tasks described in these topics:

- Choosing a Cryptographic Algorithm, Key Size, and Keystore
- Creating a Keystore
- Setting the Keystore Location
- Adding Keystore Passwords to the Credential Store
- Configuring the Policy and Credential Store

9.1.2.1 Choosing a Cryptographic Algorithm, Key Size, and Keystore

Due to algorithm restrictions with certain Java Cryptographic Extension (JCE) security providers, a number of different cryptographic algorithms and types of keystores are supported. You should choose the most appropriate cryptographic algorithm, key size, and keystore 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.

9.1.2.1.1 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

9.1.2.1.2 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.

9.1.2.2 Creating a Keystore

The `keytool` command will generate a keystore, which requires a password to open. Inside the keystore, a key, `oracle.irm.wrap`, will be stored, and access to this key requires an additional password.

To create a keystore 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 keystore.

   - 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 keystore 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 keystore 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

9.1.2.3 Setting the Keystore Location

The Rights Server configuration needs to be updated so that it can locate the keystore file. You can set the keystore location in the server configuration with either Fusion Middleware Control, on the Oracle IRM General Settings page, or with the WebLogic Scripting Tool (WLST) connect and setIRMKeyStore commands.

Note: If SSL is enabled, before you use WLST to connect to the Administration Server, you must either append the following parameters to the JVM_ARGS section of the wlst.sh file or set them in the CONFIG_JVM_ARGS environment variable:

```
-Dweblogic.security.SSL.ignoreHostnameVerification=true
-Dweblogic.security.TrustKeyStore=KeyStoreName
```

KeyStoreName is the name of the keystore in use (DemoTrust for the built-in demonstration certificate). The wlst.sh file is in the bin subdirectory of the common directory in the WebCenter Content Oracle home directory.

The suggested location for the keystore 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 keystore in this location ensures that the keystore file is backed up when the domain and corresponding credential store files are backed up.

To set the keystore location with Fusion Middleware Control:

1. Start Fusion Middleware Control at the following URL:

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

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

   ```
   http://myHost.example.com:7001/em
   ```

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

2. In the farm navigation tree on the left, expand **WebCenter Content** and **Rights**, and then click **IRM**.
3. From the **IRM** menu, select **Administration** and then **General Settings**.
4. For the keystore 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 keystore paths.
   - Keystore path for a JCEKS keystore:
     - **UNIX path:** `MW_HOME/user_projects/domains/DomainHome/config/fmwconfig/irm.jceks`
     - **Windows path:** `MW_HOME\user_projects\domains\DomainHome\config\fmwconfig\irm.jceks`
   - Keystore path for a JKS keystore:
     - **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 keystore location with WLST commands:

1. Enter the following WLST commands:

   - **UNIX operating system**

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

   - **Windows operating system**

     ```
     WCC_ORACLE_HOME\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 keystore type and keystore path.

2. For the keystore 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 keystore path, enter one of the following values.

   - Keystore path for an AES keystore:

     UNIX path: `MW_HOME/user_projects/domains /DomainHome/config/fmwconfig/irm.jceks`

     Windows path: `MW_HOME\user_projects\domains \DomainHome\config\fmwconfig\irm.jceks`

   - Keystore path for an RSA keystore:

     UNIX path: `MW_HOME/user_projects/domains/ DomainHome/config/fmwconfig/irm.jks`

     Windows path: `MW_HOME\user_projects\domains \DomainHome\config\fmwconfig\irm.jks`

9.1.2.4 Adding Keystore Passwords to the Credential Store

You must add passwords for the Oracle IRM keystore to the credential store with WLST commands. A keystore password and a password for the generated key were set when the keystore was created. These passwords are required by the Rights.

To add keystore passwords to the credential store:

- For an AES keystore, enter the following WLST commands:

  – **UNIX operating system**

  ```
  WCC_ORACLE_HOME/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**

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

  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 keystore.
  - The `"dummy"` parameter passed to the `createCred` command is the user name parameter. The keystore 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 keystore, enter the following WLST commands:

  – **UNIX operating system**

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

  – **Windows operating system**

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

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 keystore.
- The `"dummy"` parameter passed to the `createCred` command is the user name parameter. The keystore 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.

9.1.2.5 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 keystore. There are no specific configuration steps for Oracle IRM if the credential and policy stores are reassociated with an external LDAP authentication provider, as described in Section 3.9, "Reassociating the Identity Store with an External LDAP Authentication Provider."

9.2 Validating the Oracle IRM Configuration

When the Oracle IRM Managed Server is running, the Oracle IRM application is deployed to the Oracle WebLogic Server domain. You can validate that the configuration of the Managed Server was successful by accessing this URL:

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

For example:

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

9.3 Configuring the Identity Store

Oracle IRM uses OPSS to obtain user and group details from the external LDAP authentication provider. For information about configuring the identity store, see Section 3.9, "Reassociating the Identity Store with an External LDAP Authentication Provider."

9.4 Integrating Rights with Oracle Access Manager 11g

Oracle Access Manager is the recommended single sign-on (SSO) solution for Oracle WebCenter Content applications. It provides flexible and extensible authentication and authorization, as well as audit services. You can integrate Oracle IRM with Oracle Access Manager by configuring both of them for the integration.

Oracle IRM supports Basic authentication with Oracle Access Manager, which contains an authorization engine that grants or denies access to particular resources based on properties of the user requesting access as well as on the environment from which the request was made.

Oracle IRM currently has limited support for SSO through Oracle Access Manager 11*g*, as described in this section.

Public URIs need to be specified for Oracle Access Manager 11*g*:

- `/irm_rights`
- `/irm_rights/.../*`

Oracle IRM Desktop does not support Oracle Access Manager 11*g*.

You also need to protect the following URI:

- `/irm_rights/faces`

Implementation of single sign-on (SSO) with the Oracle IRM 11*g* 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 10*g* 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 10*g* and not with Oracle Access Manager 11*g* for Release 11.1.1.6.0.
- For information about Oracle Access Manager 10*g*, see the *Oracle Access Manager Access Administration Guide*.
- For information about configuring Windows Native Authentication (WNA), see "Configuring Single Sign-On with Microsoft Clients" in *Securing Oracle WebLogic Server*.

After you install and configure Oracle Access Manager 11*g*, you can configure it and Oracle IRM to work together.

Note: The following procedure should be performed only after you have installed Oracle WebCenter Content (described in Chapter 2, "Installing Oracle WebCenter Content") and configured an Oracle IRM Managed Server (described in Chapter 3, "Configuring Oracle WebCenter Content Applications"). You should also have configured and tested any required connections.

To configure Oracle IRM and Oracle Access Manager 11g to work together:

1. Install Oracle Access Manager 11*g*, as described in "Installing Oracle Identity and Access Management (11.1.1.7.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.
2. Configure Oracle Access Manager 11*g*, as described in "Configuring Oracle Access Manager" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.
3. Install and configure Oracle HTTP Server (OHS), as described in the *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 *Oracle Fusion Middleware Installing Webgates for Oracle Access Manager*.

5. Append Oracle WebCenter Content URIs to forward to the `mod_wl_ohs.conf` file, as in the following example:

```
# IRM management website
<Location /irm_rights>
      SetHandler weblogic-handler
      WebLogicHost managedServerHost
      WebLogicPort managedServerPort
</Location>
```

   In the preceding example, *`managedServerHost`* represents the host name of the machine hosting Oracle IRM, and *`managedServerPort`* represents the port number of the Oracle WebLogic Server instance hosting Oracle IRM.

   > **Note:** The entries in the preceding `Location` element are used by the web server to forward requests that match the URL pattern (for example, `/irm_rights`) to the Oracle IRM Managed Server.

   The `Location` element in the next example specifies a host and port number:

```
<Location /irm_rights>
  SetHandler weblogic-handler
  WebLogicHost irm.example.com
  WebLogicPort 16100
</Location>
```

6. Log in to the Oracle Access Manager console, as described in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*, and follow the instructions in the administrator's guide to do these tasks:

   a. Create a new Application Domain called `IRM Domain`.

   b. Select **IRM Domain**, then **Resources**, and then create entries for all the Oracle IRM URLs:

      * `/irm_rights`
      * `/irm_rights/.../*`
      * `/irm_rights/faces`
      * `/irm_rights/faces/.../*`

   c. Select **IRM Domain**, then **Authentication Policies**, and then create a Protected Policy and a Public Policy.

   d. In the Authentication Protected Policy, add these Oracle IRM resources:

      * `/irm_rights/faces`
      * `/irm_rights/faces/.../*`

   e. In the Authentication Public Policy, add these Oracle IRM resources:

      * `/irm_rights`
      * `/irm_rights/.../*`

   f. Select **IRM Domain**, then **Authorization Policies**, and then create a Protected Policy and a Public Policy.

   g. Add the same Oracle IRM protected and public resources to the Protected Policy and the Public Policy, to match the Authentication policies.

7. Configure the Oracle WebCenter Content domain by performing these tasks:

   a. Add and configure the Oracle Access Manager ID Asserter.

   b. Add and configure Oracle Internet Directory.

   c. Add the OPSS SSO provider (Oracle Access Manager).

   For more information about these tasks, see "Deploying the Oracle Access Manager 11g SSO Solution" in the *Oracle Fusion Middleware Application Security Guide*.

8. Test the Oracle Access Manager installation.

   After installing and configuring Oracle Access Manager 11*g*, check that you can access all of the configured applications and that the global login and logout is giving you access to all of your configured applications without prompting you to sign in again. Also test global logout, where available, and make sure you are logged out of all other related applications.

   For example, if `mod_wl_ohs.conf` redirects `/irm_rights` to `irm.example.com:16100` and if OHS is listening on the port `oam.example.com:7778`, then the IRM Rights application can be accessed through `https://oam.example.com:7778/irm_rights`, provided Oracle Access Manager has been set up correctly. After authentication, Oracle Access Manager will internally delegate requests to `https://irm.example:16100/irm_rights`.

9.5 Configuring Oracle IRM to Use Oracle RAC

To use Oracle RAC with an Oracle IRM instance, the Oracle IRM data source needs to be altered using the Oracle WebLogic Server Administration Console and the following procedure:

1. From **Services**, select **JDBC**, and then select **DataSources**
2. Select the Oracle IRM data source.
3. On the **Transaction** tab, check **Supports Global Transactions**, then check **Emulate Two-Phase Commit**.
4. Click **Save**.

This will set the `global-transactions-protocol` for Oracle IRM data sources for Oracle RAC to `EmulateTwoPhaseCommit`.

10 Verifying the Oracle WebCenter Content Configuration

This chapter explains how to verify the configuration of Oracle WebCenter Content and its applications.

This chapter includes the following sections:

- Section 10.1, "Starting the Administration Server"
- Section 10.2, "Starting Managed Servers"
- Section 10.3, "Restarting a Managed Server"
- Section 10.4, "Using Node Manager with Oracle WebCenter Content"
- Section 10.5, "Increasing the Java Heap Size for a Managed Server"
- Section 10.6, "Verifying the Configuration of Oracle WebCenter Content"

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.

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 Imaging Managed Server and logging in for the first time, see Section 6.1, "Completing the Initial Imaging Configuration," and do not start the Managed Server until you have completed the tasks before Section 6.1.2, "Starting the Imaging Managed Server and Accessing the Web Client."
- Before logging in to the Oracle IRM Management Console for the first time or using Content application server Desktop, see Section 9.1, "Completing the Initial Oracle IRM Configuration."

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` (WebCenter Content)
- `IBR_server1` (Inbound Refinery)
- `IPM_server1` (Imaging)
- `capture_server1` (Capture)
- `IRM_server1` (Oracle IRM)
- `URM_server1` (Records)

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

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

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

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

The value of *`admin_url`* is the Administration Server URL. This is an optional parameter. If the Administration Server does not use the default port, 7001, you need to specify a value for *`admin_url`*, such as `http://localhost:8001/`.

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

For example, the following script would start an Imaging Managed Server on a UNIX operating system:

```
cd MW_HOME/user_projects/domains/domain_name/bin
./startManagedWebLogic.sh IPM_server1 http://localhost:8001/
```

On a Windows operating system, the following script would start an Oracle IRM Managed Server on the local host:

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

To avoid prompts for a user name and password on startup after you start a Managed Server the first time, you can create a `boot.properties` file in the *`domain-home`*`/servers/`*`server-name`*`/security/` directory. This file would include the following lines:

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

The `boot.properties` file will be encrypted the first time that the Managed Server is started.

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

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 "Managing System Processes" in *Administering Oracle WebCenter Content*.

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 Using Node Manager with Oracle WebCenter Content

The Oracle WebLogic Server Node Manager enables you to start and stop WebLogic Server instances remotely, monitor them, and automatically restart them after an unexpected failure. You can configure Oracle WebCenter Content Managed Servers, the WebLogic Server Administration Server, and Node Manager to work together in a WebLogic Server domain. Node Manager is installed on all the machines that host any server instance.

Before you can use Node Manager to start and stop Oracle WebCenter Content Managed Servers in a domain, you need to do these configuration tasks:

- Configure at least one machine for the domain.
- Assign the Administration Server and Managed Servers (such as `AdminServer`, `IPM_server1`, and `UCM_server1`) to one or more machines.
- Enable Node Manager to use the Oracle WebCenter Content startup scripts by setting the `StartScriptEnabled` property in the `nodemanager.properties` file to `true`.

This section describes how to configure a machine in a WebLogic Server domain, assign the Administration Server and Managed Servers to a machine, and enable Node Manager to use startup scripts before you start it. For information about creating or extending a domain to configure Oracle WebCenter Content, see Chapter 3, "Configuring Oracle WebCenter Content Applications."

10.4.1 Configuring a Machine

The Administration Server uses a machine definition and the Node Manager application to start remote servers. During the initial configuration of Oracle WebCenter Content, you can configure machines through the Fusion Middleware Configuration Wizard. After the initial configuration, you can configure machines through the Oracle WebLogic Server Administration Console. By default the local host is preconfigured and named `LocalMachine`.

To configure a machine through the Fusion Middleware Configuration Wizard:

1. When you get to the Select Optional Configuration screen in the Fusion Middleware Configuration Wizard, be sure to select **Managed Servers, Clusters and Machines**.
2. On the Configure Machines screen, click **Add**.
3. Specify values for these fields:
   - **Name**

     Enter a valid machine name, such as **Linux-Box**. The machine name identifies the machine within the Oracle WebLogic Server domain; it does not have to match the network name for the machine. The name must be unique within the domain.
   - **Node manager listen address**

     Select a value from the drop-down list for the listen address used by Node Manager to listen for connection requests. By default, the IP addresses defined for the local system and `localhost` are shown in the drop-down list. The default value is `localhost`.

     If you specify an IP address for a machine that hosts the Administration Server and you need to access Node Manager, you must disable host name verification. For more information, see "Disabling Host Name Verification" in *Enterprise Deployment Guide for Oracle WebCenter Content*.
   - **Node manager listen port**

     Enter a valid value for the listen port used by Node Manager to listen for connection requests. The valid listen port range for Node Manager is from `1` to `65535`. The default value is `5556`.

     Note: If you are running Node Manager in a WebLogic Server domain that includes an Inbound Refinery Managed Server, the port number on one or the other needs to be configured different from the default. Node Manager and Inbound Refinery have the same default port number.

To configure a machine through the WebLogic Server Administration Console:

1. Log in to the WebLogic Server Administration Console.
2. Under **Domain Structure** on the left, expand **Environment**, and click **Machines**.
3. On the Summary of Machines screen, click **New**.
4. On the **Machine Identity** step, specify values for the following items:
   - **Name**
   - **Machine OS**

5. Click **Next**.
6. On the **Node Manager Properties** step, specify values for the following items:
   - **Type**
   - **Listen Address**
   - **Listen Port**

   Optionally, configure the debug settings.
7. Click **Finish**.

10.4.2 Assigning Servers to a Machine

Each machine definition can manage zero or more servers. During the initial configuration of Oracle WebCenter Content, you can assign the Administration Server and Managed Servers to one or more machines through the Fusion Middleware Configuration Wizard.

After the initial configuration, you can assign Managed Servers to machines through the Oracle WebLogic Server Administration Console.

To assign servers to a machine through the Fusion Middleware Configuration Wizard:

1. On the Assign Servers to Machines screen, select one or more servers in the Server area
2. Click the right arrow button to assign the selected server or servers to a machine.
3. Click **Next** when you are done.

To assign servers to a machine through the WebLogic Server Administration Console:

1. Log in to the WebLogic Server Administration Console.
2. Under **Domain Structure** on the left, expand **Environment**, and click **Machines**.
3. Click the machine name to which you would like to assign a server.
4. In the resulting Settings screen, click the **Servers** tab under **Configuration**.
5. Click **Add**.
6. In the Add a Server to Machine screen, under **Identify a Server**, choose a server to add from the list of available servers. (Optionally, you can create a new server.)
7. Click **Next** or **Finish**.

10.4.3 Enabling the Use of Startup Scripts Before Starting Node Manager

Before you start Node Manager the first time, you can run the `setNMProps.sh` script to set the `StartScriptEnabled` property to `true`. This setting is required for Node Manager to start the Managed Servers with startup scripts. You must use the `StartScriptEnabled` property to avoid class-loading failures and other problems.

If you enable Node Manager to use startup scripts on a machine that hosts one or more Managed Servers that are assigned to a machine, you can start and stop the Managed Servers remotely using the Administration Console or the command line. Node Manager can also automatically restart a Managed Server after an unexpected failure.

For a Records Managed Server, before you start Node Manager, be sure to complete the Records setup checklist, described in Section 8.1, "Completing the Initial Records Configuration."

To enable startup scripts and start Node Manager:

1. Navigate to the following directory

   ```
   MW_HOME/oracle_common/common/bin
   ```
   `MW_HOME` is the directory where Oracle Fusion Middleware is installed.

2. Run the `setNMProps.sh` script to set the `StartScriptEnabled` property to `true` before starting Node Manager:

   ```
   ./setNMProps.sh
   ```

   This is a one-time action. After you run this script, you can skip this step before starting Node Manager again.

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

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

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

   `WL_HOME` is the directory where Oracle WebLogic Server is installed.

For more information about Node Manager, see *Managing Server Startup and Shutdown for Oracle WebLogic Server* and *Node Manager Administrator's Guide for Oracle WebLogic Server*.

10.4.4 Using Node Manager to Manage Servers

You can use Oracle Node Manager to start and stop Oracle WebLogic Server instances remotely, monitor them, and automatically restart them after an unexpected failure through the WebLogic Server Administration Console.

1. Log in to the WebLogic Server Administration Console.
2. Under **Domain Structure** on the left, expand **Environment**, and click **Servers**.
3. Click the **Control** tab.
4. Select one or more servers to control.
5. Click a button corresponding to a control function.

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 Oracle JRockit JDK, increase the heap size for each Managed Server in an Oracle WebCenter Content domain to 1 GB (1024 MB). If you use Node Manager to start the Managed Servers, you can specify a heap size 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. For more information, see Section 3.5.2, "Setting the USER_MEM_ARGS Environment Variable for a Managed Server."

10.6 Verifying the Configuration of Oracle WebCenter Content

To verify the configuration of Oracle WebCenter Content, start a web browser, and enter the following URLs to test access to the Administration Server, Administration Console, and Fusion Middleware Control, as well as to applications in your Oracle WebLogic Server domain.

- To access the Administration Server:

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

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

  ```
  http://myHost.example.com:7001
  ```

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

- To access the Administration Console:

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

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

  ```
  http://myHost.example.com:7001/console
  ```

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

- To access Fusion Middleware Control:

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

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

  ```
  http://myHost.example.com:7001/em
  ```

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

  In Fusion Middleware Control, you can configure the pages for Oracle WebCenter Content applications.

- To test WebCenter Content by accessing Content Server:

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

  The default port number for WebCenter Content is `16200`.

The first user to log in to Oracle WebCenter Content Server must be the administrator of the Oracle WebLogic Server domain, to complete the configuration of Content Server. For more information, see Section 4.2, "Completing the Initial WebCenter Content Configuration,", and see also "Overview of System Administration Tasks," "Understanding Security and User Access," and "Managing System Processes" in *Administering Oracle WebCenter Content*.

- To test a newly set up Inbound Refinery instance:

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

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

- To test a newly set up Imaging instance:

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

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

  - To access the Oracle Application Extension Framework (AXF) administration console:

    `http://<Server>:16000/axf/faces/pages/axfadmin.jspx`

  - To access the Oracle Business Process Management (Oracle BPM) work list:

    `http://<Server>:8001/integration/worklistapp`

- To test a newly set up Capture instance:

  `http://`*`managedServerHost`*`:`*`managedServerPort`*`/dc-console`

  Log in with the user name and password for Oracle WebLogic Server. The default port number for Capture is `16400`.

- To test a Capture client:

  `http://`*`managedServerHost`*`:`*`managedServerPort`*`/dc-client`

  Log in with the user name and password for Oracle WebLogic Server. The default port number for Capture is `16400`.

- To test a newly set up Oracle IRM instance:

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

- To test a newly set up Records instance:

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

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

11

Uninstalling Oracle WebCenter Content

This chapter explains how to uninstall Oracle WebCenter Content from Oracle Fusion Middleware.

This chapter includes the following sections:

11.1 Preparing to Uninstall Oracle WebCenter Content

Uninstalling Oracle WebCenter Content from your system includes stopping Oracle WebLogic Server, removing application schemas, and uninstalling 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 Fusion Middleware

Before uninstalling the Oracle WebCenter Content component from Oracle Fusion Middleware, you should stop all of the servers and processes.

You can stop 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.

To stop Oracle WebLogic Server and server processes:

1. Stop each Managed Server in the Oracle WebLogic Server domain with the `stopManagedWebLogic` script:

   - **UNIX script**: *`MW_HOME`*`/user_projects/domains/`*`DomainHome`*`/bin/stopManagedWebLogic.sh` *`server_name`* `[`*`admin_url`*`]`
   - **Windows script**: *`MW_HOME`*`\user_projects\domains\`*`DomainHome\bin\stopManagedWebLogic.cmd server_name`* `[`*`admin_url`*`]`

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

   - `UCM_server1` (WebCenter Content)
   - `IBR_server1` (Inbound Refinery)
   - `IPM_server1` (Imaging)
   - `capture_server1` (Capture)
   - `IRM_server1` (Oracle IRM)
   - `URM_server1` (Records)

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

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

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

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

   The value of *`admin_url`* is the Administration Server URL. If the Administration Server does not use the default port, 7001, you need to specify a value for *`admin_url`*, such as `t3://localhost:8001/`.

   If you are prompted for the Oracle WebLogic Server user name and password, use the ones that were provided on the Configure Administrator User Name and Password screen in the configuration wizard.

2. Close any connections to the Administration Server for the domain, such as a Web browser interface, and stop the Administration Server:

   - **UNIX script:** *`DomainHome`*`/bin/stopWebLogic.sh`
   - **Windows script:** *`DomainHome`*`\bin\stopWebLogic.cmd`

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

11.3 Removing Oracle WebCenter Content Schemas

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

11.3.1 Starting the Repository Creation Utility

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

- Oracle Software Delivery Cloud at

  `http://edelivery.oracle.com/`

- Oracle Fusion Middleware 11*g* Software Downloads page on Oracle Technology Network (OTN) at

  `http://www.oracle.com/technetwork/indexes/downloads/index.html`

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

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

Start RCU with the `rcu` startup file:

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

11.3.2 Dropping Schemas

Follow these instructions to drop one or more Oracle WebCenter Content schemas:

1. Welcome screen

   Click **Next**.

2. Create Repository screen

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

3. Database Connection Details screen

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

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

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

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

4. Select Components screen

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

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

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

   After the checking is complete with no errors, click **OK** to dismiss the dialog box, and then click **Next**.

5. Summary screen

   Click **Drop**. A Drop dialog box appears, in which you can click **Stop** before the schemas are dropped.

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

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

6. Completion Summary screen

   Click **Close**.

11.4 Removing the WebCenter Content Oracle Home

The deinstaller attempts to remove the Oracle home from which it was started. Before you remove the Oracle home for Oracle WebCenter Content, be sure to stop all running processes that use this Oracle home. After you remove the software, you will no longer be able to use your Oracle WebLogic Server domain.

This procedure does not remove any Oracle WebLogic Server domains that you have created. It removes only the software in the WebCenter Content Oracle home.

Follow the instructions in Table 11–1 to uninstall Oracle WebCenter Content.

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

Table 11–1 Deinstallation Procedure

No.	Screen	Description and Action Required
1	None	Start the Oracle Fusion Middleware 11*g* WebCenter Content Installer with the `-deinstall` option from the `bin` subdirectory of the `oui` directory in your WebCenter Content Oracle home: ■ **UNIX command:** `WCC_ORACLE_HOME/oui/bin/runInstaller -deinstall` ■ **Windows command:** `WCC_ORACLE_HOME\oui\bin\setup.exe -deinstall` On a Windows operating system, you can also start the deinstallation from the **Start** menu by selecting **Programs**, then **Oracle ECM 11g - Home1**, and then **Uninstall**. The names of folders and program groups might be different on your Windows system.
2	Welcome	Click **Next** to continue.

Table 11–1 (Cont.) Deinstallation Procedure

No.	Screen	Description and Action Required
3	Deinstall Oracle Home	Verify the Oracle home you are about to uninstall. If you want to save the configuration, click the **Save** button. Then, in the Save dialog box, specify a file, and click **Save**. In the Response File Message dialog box, click **OK**. Click **Deinstall** to continue.
4	Deinstallation Progress	This screen shows the progress and status of the deinstallation. In the Warning dialog box, click **Yes** to undeploy all Oracle WebCenter Content applications and uninstall Oracle WebCenter Content from Oracle Fusion Middleware, or click **No** to undeploy the Oracle WebCenter Content applications without deleting the WebCenter Content Oracle home.
5	Deinstallation Complete	Click **Finish** to dismiss the screen.

11.4.1 Removing the WebCenter Content Oracle Home Manually on a UNIX System

If the deinstallation procedure did not remove your WebCenter Content Oracle home directory, you can use the `rm` command to manually remove the directory and all of its subdirectories on a UNIX operating system.

To remove the WebCenter Content Oracle home on a UNIX operating system:

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

   ```
   cd MW_HOME
   ```

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

   ```
   rm -rf WCC_ORACLE_HOME
   ```

11.4.2 Removing the WebCenter Content Oracle Home Manually on a Windows System

If the deinstallation procedure did not remove your WebCenter Content Oracle home directory, you can use the **Delete** command on the **File** menu and remove program groups from the **Start** menu to manually remove the directory and all of its subdirectories on a Windows operating system.

To remove the WebCenter Content Oracle home on a Windows operating system:

- In Windows Explorer, you can navigate to the `C:\`*`MW_HOME`* directory, right-click the *`WCC_ORACLE_HOME`* folder, and then choose **Delete** from the **File** menu.
- You can remove the program groups from the `Start Menu\Programs` folder, if they exist. For example, you might remove the following program groups from `C:\Documents and Settings\All Users\Start Menu\Programs`:
  - **Oracle WebLogic (BEAHOME 1)**
  - **Oracle ECM 11g - Home1**

  The names of folders and program groups might be different on your Windows system.

12

Installing and Configuring the WebCenter Content User Interface

This chapter describes how to install and configure an Oracle WebCenter Content Managed Server with the WebCenter Content user interface. This interface, for Oracle WebCenter Content Server, is based on the Oracle Application Development Framework (Oracle ADF).

This chapter includes the following sections:

12.1 About Installing and Configuring the WebCenter Content User Interface

You can configure Content Server with the WebCenter Content user interface in addition to the native 11*g* user interface, which Content Server uses by default. The WebCenter Content user interface resides in a separate domain from Content Server and runs on a different port, 16225 by default.

This separate domain requires its own Middleware home, which can reside on the same machine as the Middleware home for Content Server or on a separate machine. You could choose to have multiple instances of the WebCenter Content user interface server interact with Oracle WebCenter Content Server (previously known as Oracle UCM Content Server).

This chapter uses the following terminology:

- The first Middleware home contains Oracle WebCenter Content and is referred to as the Oracle WebCenter Content Middleware home (*WCC_MW_HOME* in directory paths).
- The first domain contains WebCenter Content and is referred to as the Oracle WebCenter Content domain (*WCC_DOMAIN* in directory paths). This domain is associated with the Oracle WebCenter Content Middleware home.
- The second Middleware home contains the WebCenter Content user interface and is referred to as the WebCenter Content user interface Middleware home (*WCCUI_MW_HOME* in directory paths).
- The second domain contains the WebCenter Content user interface and is referred to as the WebCenter Content user interface domain (*WCCUI_domain* in directory paths). This domain is associated with the WebCenter Content user interface Middleware home.

The WebCenter Content user interface domain requires its own Middleware home because changes are made to the Oracle ADF stack that are specifically required for the WebCenter Content user interface.

The two Middleware homes and domains can reside on the same host or on different hosts. The only additional requirement to run both domains on the same host is to use a different Administration Server port for each domain. To distinguish between the two Administration Server ports, this chapter refers to them as the WebCenter Content Administration Server port (*WCC_ADMINSERVER_PORT*) and the WebCenter Content user interface Administration Server port (*WCCUI_ADMINSERVER_PORT*).

To install the WebCenter Content user interface and configure it for Content Server, you need to perform these tasks:

1. Installing and Configuring Oracle WebCenter Content 11g (11.1.1.9)
2. Installing an 11.1.1.6.0 Middleware Home with Oracle ADF 11.1.2.4
3. Installing the WebCenter Content User Interface Application
4. Deploying the WebCenter Content User Interface Application to a New Domain
5. Configuring the Administrator User
6. Accessing the WebCenter Content User Interface

12.2 Installing and Configuring Oracle WebCenter Content 11g (11.1.1.9)

Before you can install and configure the WebCenter Content User Interface, you need to install and configure Oracle WebCenter Content 11*g*R1 (11.1.1.9), as these chapters describe:

- Chapter 2, "Installing Oracle WebCenter Content"
- Chapter 3, "Configuring Oracle WebCenter Content Applications"
- Chapter 4, "Completing the WebCenter Content Configuration"

You can install a new Oracle WebCenter Content 11*g*R1 (11.1.1.9.0) application or use an existing Oracle WebCenter Content 11*g*R1 (11.1.1.9.0) installation that is configured as this section describes.

All of the operations in this section pertain to the Oracle WebCenter Content Middleware home and, therefore, the Oracle WebCenter Content domain. The following steps summarize the installation and configuration procedures for Oracle WebCenter Content in the first of two Middleware homes:

1. For the first domain (in the Oracle WebCenter Content Middleware home), follow the instructions in Chapter 2, "Installing Oracle WebCenter Content," to install these products:
   - Oracle Database 11*g* Release 2
   - Repository Creation Utility (RCU)
   - Oracle WebLogic Server in a Middleware home
   - Oracle WebCenter Content 11*g* (11.1.1.9)
2. Using RCU, create the **Oracle WebCenter Content Server - Complete** schema and the **Metadata Services** (MDS) schema, as described in Section 2.2, "Creating Oracle WebCenter Content Schemas with the Repository Creation Utility."
3. Create a WebLogic Server domain that includes a WebCenter Content Managed Server (using the **Oracle Universal Content Management - Content Server** template) and, optionally, an Oracle WebCenter Content: Inbound Refinery Managed Server (using the **Oracle Universal Content Management - Inbound Refinery** template), as described in Section 3.2, "Creating an Oracle WebLogic Server Domain."
4. Configure Content Server, as the following sections describe:

   a. Section 12.2.1, "Enabling WebCenter Content User Interface Components"

      This configuration is required for using the WebCenter Content user interface.

   b. Section 12.2.2, "Setting up the Remote Intradoc Client (RIDC)"

      This configuration is required for using the WebCenter Content user interface.

   c. Section 12.2.3, "Setting Additional Content Server Parameters"

      This configuration is optional, to set up additional configuration variables and the search engine for Content Server.

   d. Section 12.2.4, "Enabling Full-Text Searching"

      This configuration is optional, to set up Oracle Text Search.

   e. Section 12.2.5, "Generating Thumbnails and Web-Viewable Renditions"

      This configuration is optional, to enhance the WebCenter Content user interface experience.

   f. Section 12.2.6, "Configuring Digital Asset Management in Content Server"

      This configuration is optional, to set up document conversions through Digital Asset Management (DAM) and Inbound Refinery.

   g. Section 12.2.7, "Configuring Extended Features in Content Server"

      This configuration is optional, to set up standard Content Server features.

12.2.1 Enabling WebCenter Content User Interface Components

Before you can use the WebCenter Content user interface, you must enable these Content Server components: AutoSuggestConfig, DynamicConverter, and FrameworkFolders. You can enable them through the Content Server Component Manager interface, as follows:

1. Log in to Content Server as a WebCenter Content administrator.
2. From the **Administration** tray or menu, choose **Admin Server**, then **Component Manager**.
3. On the Component Manager page, select all three components under **WebCenter Content UI Components**:
   - **AutoSuggestConfig**
   - **DynamicConverter**
   - **FrameworkFolders**
4. Click **Update**, and then click **OK** to confirm enabling the component.
5. Restart Content Server, as described in Section 10.3, "Restarting a Managed Server."

12.2.2 Setting up the Remote Intradoc Client (RIDC)

The WebCenter Content user interface uses the IDC socket protocol to communicate with Content Server. To enable this communication, you must set the `IntradocServerPort` and `SocketHostAddressSecurityFilter` values in the `*WCC_domain*/ucm/cs/config/config.cfg` configuration file for Content Server, in the Oracle WebCenter Content domain.

The following syntax shows how to set these values:

```
IntradocServerPort=port_number
SocketHostAddressSecurityFilter=IP addresses of permitted UI hosts separated by a
bar symbol (|)

For example:
IntradocServerPort=4444
SocketHostAddressSecurityFilter=123.456.789.0

If you want to open this up to all hosts in the network, use this setting:
SocketHostAddressSecurityFilter=*.*.*.*
```

For more information about the `config.cfg` file, see "The config Directory" in *Oracle Fusion Middleware Developing with Oracle WebCenter Content*.

12.2.3 Setting Additional Content Server Parameters

For the WebCenter Content user interface, you can also set Content Server parameters for folders and searching.

To set additional Content Server parameters:

1. From the Content Server **Administration** menu or tray, choose **Admin Server** and then **General Configuration**.
2. Select the **Enable Accounts** checkbox.

3. In the Additional Configuration Variables area, add the following parameters, if not set already, to go in the `config.cfg` file:

   - `FoldersIndexParentFolderValues=true`

     This parameter enables you to search for content within folders, including subfolders.

   - `FldEnforceFolderFileNameUniqueness=true`

     This parameter prevents folders from having a child folder with the same name as a child document.

   - `FldEnforceCaseInsensitiveNameUniqueness=true`

     This parameter makes name-uniqueness checks for folder and file names case-insensitive. It also makes path resolution case-insensitive.

   - `SearchIndexerEngineName=OracleTextSearch` or `SearchIndexerEngineName=DATABASE.METADATA`

     This parameter enables OracleTextSearch full-text searching or database metadata searching, instead of the default database full-text searching.

4. Restart the WebCenter Content Managed Server, as described in Section 10.3, "Restarting a Managed Server."

12.2.4 Enabling Full-Text Searching

For full-text searching, you need to rebuild the Content Server index using OracleTextSearch (`SearchIndexerEngineName=ORACLETEXTSEARCH` parameter).

To enable full-text searching in the WebCenter Content user interface:

1. Access Content Server with the native user interface:

   ```
   http://WCCHOST1:16200/cs
   ```

2. From the **Administration** menu or tray, choose **Admin Applets** and then **Repository Manager**.
3. Click the **Indexer** tab.
4. Under **Collection Rebuild Cycle**, click the **Start** button.
5. Deselect **Use Fast Rebuild**.
6. Click the **OK** button.

12.2.5 Generating Thumbnails and Web-Viewable Renditions

If you want to obtain thumbnail images and web-viewable renditions of files from the WebCenter Content user interface, you can configure Inbound Refinery to provide them. You can set up an Inbound Refinery provider for thumbnails and file conversions, such as PDF Export, through the native 11*g* user interface.

To configure thumbnails in Content Server:

1. Access Content Server with the native user interface:

   ```
   http://WCCHOST1:16200/cs
   ```

2. From the **Administration** menu or tray, choose **Configure Thumbnail Options**.

3. Select **Enable this server** to create the thumbnail images box.
4. Click the **Update** button.

For more information about generating thumbnails and web-viewable renditions, see "Configuring Inbound Refinery" in *Oracle Fusion Middleware Managing Oracle WebCenter Content*.

12.2.6 Configuring Digital Asset Management in Content Server

Digital Asset Management (DAM) is available through the WebCenter Content user interface. To enable the DAM user interface in Content Server, you need to enable the DigitalAssetManager, DAMConverterSupport, ContentBasket, and ZipRenditionManagement components and set up document conversion for DAM documents in Inbound Refinery.

To configure DAM in Content Server:

1. Log in to Content Server `(http://WCCHOST1:16200/cs`) as a WebCenter Content administrator.
2. Enable these components, or verify that they are enabled:
   - DigitalAssetManager
   - DAMConverterSupport
   - ContentBasket
   - ZipRenditionManagement (enabled by default)
3. Restart Content Server, as described in Section 10.3, "Restarting a Managed Server."
4. Log in to the Inbound Refinery Managed Server (`http://WCCHOST1:16250/ibr`) by default, as an administrator, and enable the DAMConverter component for DAM.
5. Restart the Inbound Refinery Managed Server, as described in Section 10.3, "Restarting a Managed Server."
6. Log in to Content Server again as an administrator to choose file formats for conversion:
   a. From the **Administration** menu or tray, choose **Admin Applets** and then **Configuration Manager**.
   b. From the **Options** menu, choose **File Formats**.
   c. For image asset formats that you want to convert to digital assets (such as **image/gif** and **image/png**, change the conversion to **Digital Media Graphics**.

For more information about configuring DAM in Content Server and the Inbound Refinery Managed Server, see "Configuring Digital Asset Manager" in *Managing Oracle WebCenter Content*.

12.2.7 Configuring Extended Features in Content Server

Some Content Server features are supported but not necessarily required by the WebCenter Content user interface. For example, Access Control Lists (ACLs) and Accounts are not configured out of the box. If these features are enabled on Content Server, however, the WebCenter Content user interface provides access to the additional functionality.

For information about enabling ACLs in Content Server, see "Managing Access Control List Security" in *Oracle Fusion Middleware Administering Oracle WebCenter Content*.

For information about enabling Accounts in Content Server, see "Managing Accounts" in *Oracle Fusion Middleware Administering Oracle WebCenter Content*.

You can set up one of the three indexing configurations for Content Server: Oracle Text Search, Database metadata, or Database full text. For more information about how to do this, see "Configuring the Search Index" in *Oracle Fusion Middleware Administering Oracle WebCenter Content*.

These standard Content Server settings are not specific to the WebCenter Content user interface. For information about other extended features in Content Server, see *Oracle Fusion Middleware Administering Oracle WebCenter Content*.

12.3 Installing an 11.1.1.6.0 Middleware Home with Oracle ADF 11.1.2.4

Install Oracle Application Development Framework (Oracle ADF) 11*g*R1 (11.1.2.4) in an 11*g*R1 (11.1.1.6.0) Middleware home with Oracle WebLogic Server. This will include installing Oracle WebLogic Server 11gR1 (10.3.6 only) to create the Middleware home followed by installing Oracle ADF and then two Oracle ADF OPatch files.

> **Note to Windows Users:** Oracle ADF 11*g*R1 (11.1.2.4) in an 11*g*R1 (11.1.1.6.0) Middleware home does *not* support Windows Server 2012 or Windows Server 2012 R2.

If your site is going to use Oracle WebCenter Content: Desktop with the WebCenter Content user interface, you also need to install a patch to support compatibility mode in Desktop 11.1.1.9.

> **Note:** You need to follow these steps exactly to enable the WebCenter Content user interface for Content Server 11.1.1.9. Even if you have Oracle Application Development Framework 11gR1 (11.1.2.4) available, you cannot use it for the WebCenter Content user interface 11.1.1.6.0 domain. Instead, you need to install Oracle ADF 11.1.1.6.0 and then upgrade it with patches to Oracle ADF 11.1.2.4.0, as the following instructions describe.

All the operations in this section pertain to the WebCenter Content user interface Middleware home and, therefore, to the WebCenter Content user interface domain. In the following commands, *`WCCUI_MW_HOME`* refers to the WebCenter Content user interface Middleware home, which includes the Oracle ADF installation.

For the WebCenter Content user interface domain, perform these steps:

1. Install Oracle WebLogic Server 11*g*R1 (10.3.6) to c a Middleware home. This will be the WebCenter Content user interface Middleware home (`WCCUI_MW_HOME`).

2. Install Oracle Application Development Framework 11*g*R1 (11.1.1.6.0) in `WCCUI_MW_HOME`:

   a. Obtain the Oracle Application Development Framework 11*g*R1 (11.1.1.6.0) media, as described in Section 1.2.2, "Software Downloads for Oracle WebCenter Content Installation and Configuration."

   b. Unzip the ZIP file containing Oracle ADF to a temporary location, `media_loc`.

   c. Run the installer, using the following command:

      * **UNIX command:**

        ```
        media_loc/Disk1/runInstaller -jreLoc JAVA_HOME
        ```

      * **Windows command:**

        ```
        media_loc\Disk1\setup.exe -jreLoc JAVA_HOME
        ```

3. Obtain the Oracle Application Development Framework 11*g*R1 (11.1.2.4.0) OPatch 16546129 (`16546129_11.1.1.6.0_Generic.zip`) from My Oracle Support (formerly Oracle*MetaLink*) at `https://support.oracle.com`.

4. Unzip the patch ZIP file into a temporary folder, `temp_location`, and run the following command:

   - **UNIX command:**

     ```
     WCCUI_MW_HOME/oracle_common/OPatch/opatch apply -jre JAVA_HOME/jre -oh
     WCCUI_MW_HOME/oracle_common/ temp_location/16546129
     ```

   - **Windows command:**

     ```
     WCCUI_MW_HOME\oracle_common\OPatch\opatch apply -jre JAVA_HOME\jre -oh
     WCCUI_MW_HOME\oracle_common\ temp_location\16546129
     ```

   In the command, `JAVA_HOME` is the location of the JDK.

5. Obtain the Oracle Application Development Framework 11*g*R1 (11.1.2.4.0) OPatch 16546157 (`p16546157_11.1.1.6.0_generic.zip`) from `https://support.oracle.com`.

6. Unzip the patch ZIP file into a temporary folder, `temp_location`, and run the following command:

   - **UNIX command:**

     ```
     WCCUI_MW_HOME/oracle_common/OPatch/opatch apply -jre JAVA_HOME/jre -oh
     WCCUI_MW_HOME/oracle_common/ temp_location/16546157
     ```

   - **Windows command:**

     ```
     WCCUI_MW_HOME\oracle_common\OPatch\opatch apply -jre JAVA_HOME\jre -oh
     WCCUI_MW_HOME\oracle_common\ temp_location\16546157
     ```

7. (Optional) For MDS customizing of the WebCenter Content user interface, obtain patch number 16020846, version 11.1.2.4.0 (`p16020846_111240_Generic.zip`), from `https://support.oracle.com`.

8. (Optional) Unzip the patch ZIP file into a temporary folder, *temp_location*, and run the following command:

   - **UNIX command:**

     ```
     WCCUI_MW_HOME/oracle_common/OPatch/opatch apply -jre JAVA_HOME/jre -oh
     WCCUI_MW_HOME/oracle_common/ temp_location/16825232
     ```

   - **Windows command:**

     ```
     WCCUI_MW_HOME\oracle_common\OPatch\opatch apply -jre JAVA_HOME\jre -oh
     WCCUI_MW_HOME\oracle_common\ temp_location\16825232
     ```

9. (Optional) For Internet Explorer 11 renditions, obtain patch number 19469801, version 11.1.2.4.0 (`p19469801_111240_Generic.zip`), from `https://support.oracle.com`.

10. (Optional) Unzip the patch ZIP file into a temporary folder, *temp_location*, and run the following command:

    - **UNIX command:**

      ```
      WCCUI_MW_HOME/oracle_common/OPatch/opatch apply -jre JAVA_HOME/jre -oh
      WCCUI_MW_HOME/oracle_common/ temp_location/19469801
      ```

    - **Windows command:**

      ```
      WCCUI_MW_HOME\oracle_common\OPatch\opatch apply -jre JAVA_HOME\jre -oh
      WCCUI_MW_HOME\oracle_common\ temp_location\19469801
      ```

11. (Optional) For Oracle ADF Help, obtain patch number 18102108, version 11.1.2.4.0 (`p18102108_111240_Generic.zip`), from `https://support.oracle.com`.

12. (Optional) Unzip the patch ZIP file into a temporary folder, *temp_location*, and run the following command:

    - **UNIX command:**

      ```
      WCCUI_MW_HOME/oracle_common/OPatch/opatch apply -jre JAVA_HOME/jre -oh
      WCCUI_MW_HOME/oracle_common/ temp_location/18102108
      ```

    - **Windows command:**

      ```
      WCCUI_MW_HOME\oracle_common\OPatch\opatch apply -jre JAVA_HOME\jre -oh
      WCCUI_MW_HOME\oracle_common\ temp_location\18102108
      ```

12.4 Installing the WebCenter Content User Interface Application

The WebCenter Content user interface artifacts are in a ZIP file called `WccADFUI.zip`, which you can obtain from the WebCenter Content Oracle home in the Oracle WebCenter Content (first) Middleware home. The file location is `WCC_ORACLE_HOME/ucm/Distribution/WccADFUI/WccADFUI.zip`.

This ZIP file includes these WebCenter Content user interface artifacts:

- The application EAR file, `WccAdf.ear`
- The domain extension configuration template
- Custom Oracle Weblogic Scripting Tool (WLST) commands for managing the connections to Oracle WebCenter Content Server
- Support scripts for deployment and management of the application

To install the WebCenter Content user interface application:

1. Create the directory *WCCUI_MW_HOME*/oracle_common/webcenter/wccadf, in the WebCenter Content user interface (second) Middleware home.
2. Copy the *WCC_ORACLE_HOME*/ucm/Distribution/WccADFUI/WccADFUI.zip file to the *WCCUI_MW_HOME*/oracle_common/webcenter/wccadf directory.
3. Expand the ZIP file in the *WCCUI_MW_HOME*/oracle_common/webcenter/wccadf directory.

12.5 Deploying the WebCenter Content User Interface Application to a New Domain

You need to deploy the WebCenter Content user interface application to a new WebLogic Server domain before you can use the application with the Content Server application in the Oracle WebCenter Content domain. After configuration of both domains is complete, you can use either the WebCenter Content user interface or the native 11*g* user interface with Content Server.

All of the operations in this section pertain to the WebCenter Content user interface Middleware home and, therefore, to the WebCenter Content user interface domain.

To deploy the WebCenter Content user interface application:

1. Register the Oracle Metadata Services (MDS) repository in the WebCenter Content user interface application:

   a. Run WLST from the WebCenter Content user interface Middleware home:

      – **UNIX command:**

      ```
      WCCUI_MW_HOME/oracle_common/common/bin/wlst.sh
      ```

      – **Windows command:**

      ```
      WCCUI_MW_HOME\oracle_common\common\bin\wlst.cmd
      ```

   b. Run the following commands in offline mode:

      ```
      wls:/offline> archive = getMDSArchiveConfig('WCCADF_EAR_LOCATION')

      wls:/offline> archive.setAppMetadataRepository(repository='mds-mds_repo_
      name', partition='partition_name', type='DB', jndi='jdbc/mds/mds_repo_
      name')

      wls:/offline> archive.save()
      ```

      In the getMDSArchiveConfig command, *WCCADF_EAR_LOCATION* is the directory where the WccADFUI.zip file was expanded, *WCCUI_MW_HOME*/oracle_common/webcenter/wccadf.

      In the archive.setAppMetadataRepository command, *mds_repo_name* is the name of the repository, and *partition_name* is a name for the partition to be created.

   For example:

   ```
   archive =
   getMDSArchiveConfig("/user/ADFMW/oracle_common/webcenter/wccadf/WccAdf.ear")
   archive.setAppMetadataRepository(repository='mds-WCCUIMDSREPO', partition='MDS_
   PARTITION', type='DB', jndi='jdbc/mds/WCCUIMDSREPO')
   archive.save()
   ```

2. In the WebCenter Content user interface Middleware home, place the WebCenter Content user interface domain template, `oracle.ucm.cs_adf_template_11.1.1.jar`, in the following directory:

   ```
   WCCUI_MW_HOME/oracle_common/common/templates/applications/
   ```

3. Run the configuration wizard in this Middleware home:

   ```
   WCCUI_MW_HOME/oracle_common/common/bin/config.cmd
   ```

4. Create a new Weblogic Server domain, *WCCUI_DOMAIN*, using the following template:

   Oracle WebCenter Content - Web UI - 11.1.1.0

   Dependent components (JRF and EM) will be automatically enabled. This will create a new domain and a Managed Server for the WebCenter Content user interface application. You will not need any data sources to be set up for this application.

5. Upgrade the Oracle ADF shared libraries in the WebCenter Content user interface domain to Sherman Update 2:

   a. Run WLST from *WCCUI_MW_HOME*`/oracle_common/common/bin/wlst.sh`.

   b. Run the following command in offline mode:

   ```
   wls:/offline> upgradeADF('DOMAIN_HOME');
   ```

   For example:

   ```
   wls:/offline> upgradeADF('/user/ADFMW/Middleware/user_
   projects/domains/WCCUI_domain')
   Target Library "jsf#2.0@1.0.0.0_2-0-2" to JRF "AdminServer"
   Target Library "jsf#2.0@1.0.0.0_2-0-2" to JRF "WCCADF_server1"
   ```

6. Register the target Managed Server with the MDS repository, and create the metadata partition:

   a. Start the Oracle WebLogic Server Administration Server in the WebCenter Content user interface domain, which is in the WebCenter Content user interface Middleware home (*WCCUI_MW_HOME*), as described in Section 10.1, "Starting the Administration Server."

   If you have installed both domains on the same host, the port for the Administration Server in the WebCenter Content user interface domain will *not* be the default Administration Server port.

   b. Run WLST from *WCCUI_MW_HOME*`/oracle_common/common/bin/wlst.sh`, and connect to the WebLogic Server instance in interactive mode:

   ```
   wls:/offline> connect()
   Please enter your username : weblogic
   Please enter your password :

   Please enter your server URL: [t3://localhost:7001] :t3://host:port of
   admin server where the WebCenter Content user interface Managed Server is
   running
   ```

c. Run the following commands:

```
wls:/mydomain/serverConfig> registerMetadataDBRepository('mds_repo_name',
'Oracle', 'db_host_name', 'db_port_number', 'db_name', 'mds_schema_
username', 'mds_schema_password', 'target_server')

wls:/mydomain/serverConfig> createMetadataPartition(repository='mds-mds_
repo_name', partition='partition_name')
```

The target server in the preceding command is the WebCenter Content user interface Managed Server.

For example:

```
registerMetadataDBRepository('WCCUIMDSREPO', 'Oracle','my_db_server',
'1521', 'my_db', 'WCCUI_MDS', 'password', 'WCCADF_server1')
createMetadataPartition(repository='mds-WCCUIMDSREPO', partition='MDS_
PARTITION')
```

If you are upgrading an Oracle WebCenter Content 11.1.1.9.0 installation that was previously configured to work with the WebCenter Content user interface, the *mds_repo_name* and *partition_name* values should be the same as the *mds_repo_name* and *partition_name* values created during the installation of Oracle WebCenter Content 11.1.1.9.0. You can obtain these values from the Fusion Middleware Control URL of the 11.1.1.9.0 installation.

7. Restart the Administration Server in the WebCenter Content user interface domain, by stopping and then starting it, as described in Part 10.3, "Restarting a Managed Server."

   If you have installed both domains on the same host, the port for the Administration Server in the WebCenter Content user interface domain will *not* be the default Administration Server port.

8. Start the WCCADF_server1 Managed Server in the WebCenter Content user interface domain.

9. Associate the WebCenter Content user interface with Content Server through the connection architecture:

   a. Set the variable *WL_HOME* to the location of the WebLogic Server instance. For example:

```
WL_HOME=WCCUI_MW_HOME/wlserver_10.3
```

   b. Go to *WCCUI_MW_HOME*/oracle_common/webcenter/wccadf/ConnArchWlstResources/common/bin.

   c. Run the custom WLST command manageconnwlst.sh, which is present in this directory:

```
./manageconnwlst.sh

wls:/offline> connect()

Please enter your username :weblogic

Please enter your password :

Please enter your server URL [t3://localhost:7001] :t3://host:port of
WebCenter Content user interface Managed Server
```

d. Update the RIDC connection to the WebCenter Content user interface Managed Server:

```
wls:/mydomain/serverConfig>updateRIDCConnection('ADF_UI_APP_
NAME','WccAdfDefaultConnection',connUrl='idc://contentserver_host:intradoc_
port',credUsername='ucm_admin_user')
```

In the command, `ADF_UI_APP_NAME` is the **Oracle WebCenter Content - Web UI** application.

For example:

```
connect('weblogic','password','t3://myuihost.example.com:16225')
updateRIDCConnection('Oracle WebCenter Content - Web UI',
'WccAdfDefaultConnection',connUrl='idc://mycshost.example.com:4444',
credUsername='weblogic')
```

At this point the WebCenter Content user interface application instance has been set up and associated with the WebCenter Content Managed Server that was installed on the first machine.

Note: This is an IDC-based mechanism for connecting to Content Server. If you want to try a different connection mechanism, see Section 12.8, "Associating the WebCenter Content User Interface with Content Server."

10. Restart the Content Server Managed Server, as described in Section 10.3, "Restarting a Managed Server."
11. Restart the WebCenter Content user interface Managed Server.

12.6 Configuring the Administrator User

Content Server and the WebCenter Content user interface will need to access the same user directory. Standard LDAP offerings such as Oracle Internet Directory and Active Directory can be shared across domains. You can choose to configure a single sign-on solution using Oracle Access Manager or Oracle Single Sign-On, using the standard guidelines for such integration.

For more information about LDAP options, see Section 3.9, "Reassociating the Identity Store with an External LDAP Authentication Provider."

Out of the box, the WebCenter Content user interface requires one WebCenter Content administrator user to function:

- The administrator user was specified in the `credUsername` parameter of the `updateRIDCConnection()` WLST command that was used to connect to the WebCenter Content user interface Managed Server, in Section 12.5, "Deploying the WebCenter Content User Interface Application to a New Domain," Step 9d.
- You will need a user with the chosen name in the LDAP store or stores. Without this administrator user, the WebCenter Content user interface deployment will not work.
- The user must have `Administrators` rights for the WebCenter Content Managed Server.

12.7 Accessing the WebCenter Content User Interface

You can access the WebCenter Content user interface through the following URL:

```
http://wccui-host:wccui-port/wcc
```

The WebCenter Content user interface application runs on port 16225 by default.

12.8 Associating the WebCenter Content User Interface with Content Server

You can configure a JAX-WS, IDCS, IDC, HTTP, or HTTPS connection between the WebCenter Content user interface Managed Server and Content Server, to associate the WebCenter Content user interface with Content Server. The following topics describe how to configure these connections:

- Configuring a JAX-WS Connection from the WebCenter Content User Interface Server to Content Server
- Configuring a Secured Connection from the WebCenter Content User Interface Server to Content Server
- Configuring an IDCS Connection from the WebCenter Content User Interface Server to Content Server
- Configuring an IDC Connection from the WebCenter Content User Interface Server to Content Server
- Configuring an HTTP Connection from the WebCenter Content User Interface Server to Content Server
- Configuring an HTTPS Connection to Content Server Without a Certificate
- Setting Connection Attributes Through Fusion Middleware Control

12.8.1 Configuring a JAX-WS Connection from the WebCenter Content User Interface Server to Content Server

To configure a JAX-WS connection to Content Server:

1. Ensure that Metadata Services (MDS) schemas have been created in Oracle Database 11*g* Release 2 by the Repository Creation Utility (RCU).

   Create one MDS schema for the Oracle WebCenter Content domain and one MDS schema for the WebCenter Content user interface domain. For information about creating schemas, see Section 2.2, "Creating Oracle WebCenter Content Schemas with the Repository Creation Utility."

2. Apply the WSM Policy Manager Template to both the Oracle WebCenter Content domain and the WebCenter Content user interface domain, if the domain does not already have this template. The template is in this file:

   ```
   MW_HOME/oracle_common/common/templates/applications/oracle.wsmpm_template_
   11.1.1.jar
   ```

   If the file is not in the `MW_HOME/oracle_common/common/templates/applications` directory, you can extend the domain with the template.

To extend a domain with the WSM Policy Manager Template:

- **a.** If a Managed Server in the domain that you are planning to extend is running, stop it through the Administration Console.
- **b.** Launch an Oracle WebLogic Scripting Tool (WLST) shell in offline mode.
- **c.** Run the following commands in sequence:

```
wls:/offline> readDomain(r'${DOMAIN_HOME}')

addTemplate(r'${MW_HOME}/oracle_common/common/templates/applications
/oracle.wsmpm_template_11.1.1.jar')

updateDomain()

closeDomain()

exit()
```

The `addTemplate.cmd` command creates a dummy schema.

3. Restart the Administration Servers in both domains.
4. For each domain, update the `mds-owsm` JDBC connection pool to point to the MDS schema for the domain. The targets should be the Administration Server and all Oracle ADF servers. The update can be done from **Services > Data sources > mds-owsm** in the Administration Console.

   After updating a domain, restart the corresponding Administration Server. Confirm that **Monitoring > Testing > Check** data source is giving zero errors. A success message is expected, like "`Test of mds-owsm on server AdminServer was successful.`"

   > **Note:** Use separate schemas for ADF UI connection architecture and ADF UI OWSM.

   Confirm that the `wsm-pm` application is shown as `Active` on the Deployments page of the Administration Console for each domain.
5. Restart the Managed Servers in both domains.
6. Create a policy set for the WebCenter Content user interface domain:
   - **a.** In Oracle Enterprise Manager 11*g* Fusion Middleware Control, expand **WebLogic Domain** in the navigation tree on the left, and then click the name of the domain.
   - **b.** From the **WebLogic Domain** drop-down menu at the top of the domain page, choose **Web Services**, then **Policy Sets**.
   - **c.** From the **Type of Resources** menu under **Policy Set Summary**, choose **Web Service Client**, enter a name for the policy set in the **Name** field, and click **Create**.
   - **d.** Make sure the policy set is enabled.
   - **e.** Under the scope, enable the policy set, enter the name of the domain in the **Domain Name** field, and then attach a policy, such as `oracle/wss10_saml_token_client_policy`.

7. Create a policy set for the Oracle WebCenter Content domain:

   a. In Fusion Middleware Control, expand **WebLogic Domain** in the navigation tree on the left, and then click the name of the domain.

   b. From the **WebLogic Domain** drop-down menu at the top of the domain page, choose **Web Services**, then **Policy Sets**.

   c. From the **Type of Resources** menu under **Policy Set Summary**, choose **Web Service Endpoint**, enter a name for the policy set in the **Name** field, and click **Create**.

   d. Make sure the policy set is enabled.

   e. Under the scope, enter the name of the domain in the **Domain Name** field, and then attach a policy, such as `oracle/wss_saml_or_username_token_service_policy`.

8. To expedite applying the policy changes, restart the servers.

9. Confirm that the WebCenter Content web service has the GPA policy applied by inspecting the WSDL, at the following URL:

   ```
   http://WCC_HOST:WCC_PORT/idcnativews/IdcWebLoginPort?WSDL
   ```

   For example:

   ```
   http://slc05amp.example.com:16200/idcnativews/IdcWebLoginPort?WSDL
   ```

   In the WSDL, check for this code:

   ```
   wsp:PolicyReference xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
   URI="#wss_saml_or_username_token_service_policy" wsdl:required="false"/>
   ```

10. To do an identity switch over the top of a standard SAML identity propagation policy, you need to be able to override subject precedence from its default value of `true`, to be `false` instead.

    This instructs the server not to automatically send the connected subject, but rather allow it to explicitly set the identity that should be sent across.

    The connection architecture has a Boolean property that you can set to activate an RIDC filter that results in `requestContext.put(ClientConstants.WSM_SUBJECT_PRECEDENCE, "false")` being set.

    > **Note:** If a Credential map exists, ensure that the `password` property (`oracle.wcc.ridc.credential.password`) is cleared from the Credential map before executing the following command. To check this property in Fusion Middleware Control, go to the WebCenter Content user interface page, and from the **WebLogic Server** drop-down menu, choose **Security**, then **Credentials**, then **WccAdf.oracle.wcc.adf**, and then **anonymous#WccAdfDefaultConnection**. To clear the property, click **Edit**, remove `oracle.wcc.ridc.credential.password`, and save the change.

To activate the RIDC filter, run the following command:

```
updateRIDCConnection('Oracle WebCenter Content - Web UI',
'WccAdfDefaultConnection',
connUrl="http://slc05elc.example.com:16200/idcnativews",
jaxwsRegisteridentityswitchfilter="true",credImpersonationAllowed='false')
```

Run the following Connection Architecture command:

```
displayRIDCConnection('Oracle WebCenter Content - Web UI',
'WccAdfDefaultConnection')
```

Now the Connection Architecture attributes should look as follows:

```
PropConnectionUrl = http://WCCUI_HOST:16200/idcnativews
PropConnectionSocketTimeout = null
PropConnectionPoolMethod = null
PropConnectionPoolSize = null
PropConnectionWaitTime = null
PropCredentialUsername = weblogic
PropCredentialAppIdKey = null
PropCredentialImpersonationAllowed = null
PropProtocolJaxWSStack = null
PropProtocolJaxWSPolicy = null
PropProtocolJaxWSJpsConfigFile = null
PropProtocolJaxWSSkipStackOptimize = null
PropProtocolJaxWSServerInsName = null
PropProtocolJaxWSRegisterIdentitySwitchFilter = true
PropProtocolHttpLibrary = null
PropProtocolIdcsAlgorithm = null
PropProtocolIdcsKeystoreFile = null
PropProtocolIdcsKeystoreAlias = null
PropProtocolIdcsTrustManagerFile = null
```

Note: Make sure `PropCredentialImpersonationAllowed` is set to `null` or `false`, not to `true`.

11. For an application to switch identity, grant it a special policy-code grant in the `system-jazn-data.xml` file, under `*WCCUI_MW_HOME*/user_projects/domains/*WCCUI_domain*/config/fmwconfig`. Change the name, as in the following code:

```
<grant>
   <grantee>
     <codesource>
       <url>file:${common.components.home}/modules/oracle.wsm.agent.
       common_11.1.1/wsm-agent-core.jar</url>
     </codesource>
   </grantee>
   <permissions>
     <permission>
       <class>oracle.wsm.security.WSIdentityPermission</class>
       <name>resource=Oracle WebCenter Content - Web UI</name>
       <actions>assert</actions>
     </permission>
   </permissions>
</grant>
```

12. Restart the WebCenter Content user interface Managed Server.

12.8.2 Configuring a Secured Connection from the WebCenter Content User Interface Server to Content Server

An SSL Incoming Provider is leveraged and instantiated to create an SSL server socket to which Intradoc clients can connect, and whereby traffic is encrypted.

The provider can be configured with or without requiring client authentication (the WebCenter Content user interface Managed Server is a client of Content Server).

When client authentication is *not* required, the JAVA RIDC client making the connection to the SSL server socket (Intradoc secure-socket port) does not need to present a valid certificate. This mode is not very different from a normal, non-SSL Intradoc connection. The main difference, however, is that traffic is encrypted and cannot be viewed by packet capture, and so on, in the clear.

Client authentication means that the client must supply a valid SSL certificate signed by an authority that is in the server's trust store. In this context, client authentication is not tied to any particular end user, but rather to the Java client program.

When the `Require Client Authentication` option is selected for the provider, and a secure Intradoc connection is made by the Java RIDC client to Content Server, a client that does not present a valid certificate will receive an exception, such as this one:

```
javax.net.ssl.SSLHandshakeException: Received fatal alert: bad_certificate
oracle.stellent.ridc.protocol.ProtocolException:
javax.net.ssl.SSLHandshakeException: Received fatal alert: bad_certificate
at
oracle.stellent.ridc.protocol.intradoc.HdaProtocol.readResponse(HdaProtocol.java:2
57)
at oracle.stellent.ridc.IdcClient.sendRequest(IdcClient.java:184)
at Ping.ping(Ping.java:42)
at Ping.main(Ping.java:20)
Caused by: javax.net.ssl.SSLHandshakeException: Received fatal alert: bad_
certificate
at com.sun.net.ssl.internal.ssl.Alerts.getSSLException(Alerts.java:174)
at com.sun.net.ssl.internal.ssl.Alerts.getSSLException(Alerts.java:136)
at com.sun.net.ssl.internal.ssl.SSLSocketImpl.recvAlert(SSLSocketImpl.java:1720)
at com.sun.net.ssl.internal.ssl.SSLSocketImpl.readRecord(SSLSocketImpl.java:954)
at
com.sun.net.ssl.internal.ssl.SSLSocketImpl.performInitialHandshake(SSLSocketImpl.j
ava:1138)
at
com.sun.net.ssl.internal.ssl.SSLSocketImpl.readDataRecord(SSLSocketImpl.java:753)
at com.sun.net.ssl.internal.ssl.AppInputStream.read(AppInputStream.java:75)
at java.io.BufferedInputStream.fill(BufferedInputStream.java:218)
at java.io.BufferedInputStream.read(BufferedInputStream.java:237)
at oracle.stellent.ridc.common.util.StreamUtil.readRawLine(StreamUtil.java:227)
at oracle.stellent.ridc.common.util.StreamUtil.readLine(StreamUtil.java:254)
at
oracle.stellent.ridc.protocol.intradoc.HdaProtocol.readHeaders(HdaProtocol.java:45
9)
at
oracle.stellent.ridc.protocol.intradoc.HdaProtocol.readResponse(HdaProtocol.java:2
15)
```

If your client (the WebCenter Content user interface Managed Server) receives such an exception, first make sure that the *WCC_domain*/ucm/cs/config/config.cfg file has SocketHostAddressSecurityFilter correctly set. The SocketHostAddressSecurityFilter value includes the IP address of the client machine; for example:

```
#hostname -i :- 10.229.187.227

SocketHostAddressSecurityFilter=10.229.187.227|127.0.0.1|0:0:0:0:0:0:0:1
```

Failure to set SocketHostAddressSecurityFilter correctly will result in an exception such as StatusMessage: Unable to establish connection to the server. Permission denied. Address '10.187.109.243' is not an allowable remote socket address.

Setting IntradocServerPort=*XXXX* is not required. Setting this property allows for non- SSL/nonencrypted Intradoc connections to this particular port from machines in the preceding trusted IP address list.

> **Caution:** If you want only SSL Intradoc connections with client-certificate authentication, but you inadvertently set IntradocServerPort, the client could go through this back door (assuming its IP address is in the trusted list).

12.8.3 Configuring an IDCS Connection from the WebCenter Content User Interface Server to Content Server

You can configure an IDC secured (IDCS) connection with or without Require Client Authentication. The WebCenter Content user interface Managed Server is a client of Content Server.

To configure an IDC secured connection with **Require Client Authentication**:

1. In the Oracle WebCenter Content domain, make the following changes, in a bash environment:

   a. Enter the following command to set the domain environment:

   ```
   source WCCUI_DOMAIN_HOME/bin/setDomainEnv.sh
   ```

   b. Create a directory named sslkeepaliveincomingprovider:

   ```
   mkdir -p $WCC_DOMAIN_
   HOME/ucm/cs/data/providers/sslkeepaliveincomingprovider

   cd $WCC_DOMAIN_HOME/ucm/cs/data/providers/sslkeepaliveincomingprovider
   ```

   You can use a different name, as long as the directory name matches the provider name specified in Step 2d.

   c. Use the CertGen utility to create a server key-certificate pair signed by the demo CA cert CertGenCA, as follows:

   ```
   java utils.CertGen -certfile ServerPublicCert -keyfile ServerPrivKey
   -keyfilepass password -cn "`hostname -f`"
   ```

   d. Create a server keystore with the server key-certificate pair.

   ```
   java utils.ImportPrivateKey -keystore keystore.jks -storepass password
   -certfile ServerPublicCert.der -keyfile ServerPrivKey.der -keyfilepass
   password -alias serverkey -keypass password
   ```

e. Add the root CA to the server keystore, using the keytool utility:

```
keytool -importcert -file $WL_HOME/server/lib/CertGenCA.der -keystore
keystore.jks -storepass password -noprompt
```

The alias is not provided in the preceding command because it will be imported under the alias name `mykey`.

f. Add the root CA to the trust keystore:

```
keytool -importcert -file $WL_HOME/server/lib/CertGenCA.der -keystore
truststore.jks -storepass welcome1 -noprompt
```

The alias is not provided in the preceding command because it will be imported under the alias name `mykey`.

2. In Oracle WebCenter Content Server, add a provider:

   a. Log in to the WebLogic Content user interface for Content Server, using the administrator user name and password.

   b. From the **Administration** tray or menu, choose **Providers**.

   c. On the Providers page, in **Provider Type** column of the **Create a New Provider** table, click **sslincoming** and then **Add** in the **Action** column of the same row.

   d. On the Add Incoming Provider page, enter or keep the following field values:

   – **Provider Name**: `sslkeepaliveincomingprovider` (or the name of the directory created in Step 1b.)

   – **Provider Description**: `For testing RIDC over SSL`

   – **Provider Class**: `idc.provider.ssl.SSLSocketIncomingProvider`

   – **Connection Class**: `idc.provider.KeepaliveSocketIncomingConnection`

   – **Server Thread Class**: `idc.server.KeepaliveIdcServerThread`

   – **Server Port**: `9995`

   – **Require Client Authentication**: `Select.`

   – **Keystore File Path**: Select `Use Default` (This value specifies `$WCC_DOMAIN_HOME/ucm/cs/data/providers/sslkeepaliveincomingprovider/keystore.jks`)

   – **Keystore Password**: *`password`*

   – **Alias**: `serverkey`

   – **Alias Password**: *`password`*

   – **Truststore File Path**: Select `Use Default` (This value specifies `$WCC_DOMAIN_HOME/ucm/cs/data/providers/sslkeepaliveincomingprovider/truststore.jks`)

   – **Truststore Password**: *`password`*

   e. Click the **Add** button at the bottom of the page.

   f. Restart the WebCenter Content Managed Server.

3. Verify the *WCC_DOMAIN_HOME*/ucm/cs/data/providers/sslkeepaliveincomingprovider/provider.hda file that gets generated. It should contain the following text:

Example 12–1 Contents of the provider.hda File

```
- note passwords in clear!!
cat provider.hda
<?hda version="11gR1-11.1.1.7.0-idcprod1-120807T112220" jcharset="UTF8"
encoding="utf-8"?>
@Properties LocalData
=I
ncomingThread=idc.server.KeepaliveIdcServerThread
IntradocServerHostName=
KeystoreAlias=serverkey
KeystoreAliasPassword=password
KeystoreFile=/u01/app/oracle/product/Middleware/user_projects/domains/base_dom
ain/ucm/cs/data/providers/sslkeepaliveincomingprovider/keystore.jks
KeystorePassword=password
NeedClientAuth=
PasswordScope=sslkeepaliveincomingprovider
ProviderClass=idc.provider.ssl.SSLSocketIncomingProvider
ProviderConfig=
ProviderConnection=idc.provider.KeepaliveSocketIncomingConnection
ProviderType=sslincoming
ServerPort=9995
TruststoreFile=/u01/app/oracle/product/Middleware/user_projects/domains/base_do
main/ucm/cs/data/providers/sslkeepaliveincomingprovider/truststore.jks
TruststorePassword=password
UseDefaultKeystoreFile=1
UseDefaultTruststoreFile=1
WantClientAuth=
blDateFormat=M/d{/yy}{ h:mm[:ss]{ a}}!mAM,PM!tPST8PDT
@end
```

4. From the WebCenter Content user interface Managed Server machine, make the following changes (if you are requiring client authentication).

   a. Enter the following command to set the domain environment:

   ```
   source WCCUI_DOMAIN_HOME/bin/setDomainEnv.sh
   ```

   b. Go to the user home directory:

   ```
   cd /home/user
   ```

   c. Use the CertGen utility to create a client key-certificate pair signed by the demo CA cert `CertGenCA`, as follows:

   ```
   java utils.CertGen -certfile ClientPublicCert -keyfile ClientPrivKey
   -keyfilepass password [-cn "`hostname -f`"]
   ```

   Note: The optional `-cn` argument determines the common name to which the certificate is issued. If this argument is skipped, the certificate is issued to the host name of the machine from which the certificate is generated.

d. Create a client keystore for the WebCenter Content user interface Managed Server, with the client key-certificate pair:

```
java utils.ImportPrivateKey -keystore keystore.jks -storepass password
-certfile ClientPublicCert.der -keyfile ClientPrivKey.der -keyfilepass
password -alias clientkey -keypass password
```

e. Add the root CA to the client keystore, using the keytool utility:

```
keytool -importcert -file WCCUI_WL_HOME/server/lib/CertGenCA.der -keystore
keystore.jks -storepass password -noprompt
```

5. Connect to the WebCenter Content user interface Managed Server.
6. Run the following `updateRIDCConnection()` command, on one line:

```
updateRIDCConnection('Oracle WebCenter Content - WebUI',
'WccAdfDefaultConnection',connUrl='idcs://adc2120610.example.com:9995',
credUsername='weblogic',idcsKeystoreFile='/home/user/keystore.jks',
idcsKeystorePassword='password',idcsKeystoreAlias='clientkey',idcsKeystoreAlias
Password='password')
```

After the preceding command is run, the `cwallet.sso` file is updated under `/users/username/AppData/Roaming/JDeveloper/system11.1.2.2.39.61.83.1/DefaultDomain/config/fmwconfig`. The `cwallet.sso` file contains the password, as follows (decrypted content):

```
### Map: WccAdf.oracle.wcc.adf
1. + Key: anonymous#WccAdfDefaultConnection
class = oracle.security.jps.internal.credstore.GenericCredentialImpl
desc = null
type = java.util.Hashtable
cred = (oracle.wcc.ridc.protocol.idcs.keystore.alias.password, password)
cred = (oracle.wcc.ridc.protocol.idcs.keystore.password, password)
expires = null
```

7. Restart the WebCenter Content user interface Managed Server.

To configure an IDC secured connection without **Require Client Authentication** (only Content Server changes required):

1. Make the preceding changes to Content Server.
2. Connect to the WebCenter Content user interface Managed Server.
3. Run the following `updateRIDCConnection()` command, on one line:

```
updateRIDCConnection('Oracle WebCenter Content - Web UI',
'WccAdfDefaultConnection',connUrl='idcs://adc2120610.example.com:9995',
credUsername='weblogic')
```

4. Ensure all other parameters are unset by running the `displayRIDCConnection('Oracle WebCenter Content - Web UI','WccAdfDefaultConnection') cmd`.
5. Restart the WebCenter Content user interface Managed Server.

6. If you encounter the following error message, you need to import a certificate from the Content domain into the Oracle WebCenter Content user interface domain:

   ```
   Caused By: javax.net.ssl.SSLHandshakeException:
   sun.security.validator.ValidatorException: PKIX path building failed:
   sun.security.provider.certpath.SunCertPathBuilderException: unable to find
   valid certification path to requested target
   ```

   This error means the certificate present in the WebLogic Server trusted store for the WebCenter Content Managed Server does not match or contain the `<cacerts>` entry present in WebLogic Server trusted store for Content Server). To import this certificate and add it to the trusted keystore in the WebCenter Content user interface domain:

   a. Export the Content Server certificate as `root.cer`:

      ```
      keytool -export -file root.cer -keystore keystore_path
      ```

      In the preceding command, *`keystore_path`* is the keystore that was configured on the sslaliveincominprovider page in Content Server. For example:

      ```
      /user/11.1.1.9.0/mw9977/user_projects/domains/wccucm_
      domain/ucm/cs/data/providers/sslkeepaliveincomingprovider/keystore.jks
      ```

   b. Enter the corresponding keystore password: *`password`*

   c. Import `root.cer` into the client:

      ```
      Keytool -import -keystore <cacerts> -file root.cer
      ```

      In the preceding command, `<cacerts>` is the Java Standard Trust Keystore that was specified for the WebCenter Content user interface Managed Server in the Administration Console. For example:

      ```
      keytool -import -keystore jdk_location/jre/lib/security/cacerts -file
      root.cer
      ```

   d. If you are prompted for a password after running the preceding `keytool` command, you can enter the common password for a keystore.

   e. Restart the Web Center Content user interface Managed Server.

12.8.4 Configuring an IDC Connection from the WebCenter Content User Interface Server to Content Server

For an IDC connection to Content Server, the WebCenter Content user interface application is authenticated based on an IP address. Therefore, you need to make sure the *`WCC_DOMAIN_HOME`*`/ucm/cs/config/config.cfg` file has `SocketHostAddressSecurityFilter` set correctly.

`SocketHostAddressSecurityFilter` includes the IP address of the client machine (the WebCenter Content user interface machine); for example:

```
#hostname -
i :- 10.229.187.227
SocketHostAddressSecurityFilter=10.229.187.227|127.0.0.1|0:0:0:0:0:0:0:1
```

To configure an IDC connection to Content Server:

1. Connect to the WebCenter Content user interface.
2. Run the following `updateRIDCConnection()` command, on one line:

   ```
   updateRIDCConnection('Oracle WebCenter Content - Web UI',
   'WccAdfDefaultConnection',connUrl='idc://adc2120610.example.com:4444',
   credUsername='weblogic')
   ```

   The port number `4444` is the `IntradocServerPort` value for Content Server.
3. Restart the WebCenter Content user interface Managed Server.

12.8.5 Configuring an HTTP Connection from the WebCenter Content User Interface Server to Content Server

To configure an HTTP connection to Content Server:

1. Connect to the WebCenter Content user interface.
2. Run the following `updateRIDCConnection()` command, on one line:

   ```
   updateRIDCConnection('Oracle WebCenter Content - Web UI',
   'WccAdfDefaultConnection',connUrl='http://adc2120610.example.com:7777/cs
   /idcplg',credUsername='weblogic',credPassword='password',
   httpLibrary='oracle',credImpersonationAllowed='true')
   ```

3. Restart the WebCenter Content user interface Managed Server.

12.8.6 Configuring an HTTPS Connection to Content Server Without a Certificate

To configure an HTTPS connection to Content Server without a certificate:

1. Enable the SSL listen port in the WebLogic Server Administration Console. For example:

   SSL listen port: 16201

2. Update the following two entries in the Content Server configuration file, `config.cfg`, under *`WCC_MW_HOME`*`/user_projects/domains/cs_domain/ucm/cs/config`:

   ```
   HttpServerAddress=adc2120610.example.com:16201
   UseSSL=Yes
   ```

3. Restart the Oracle WebCenter Content Managed Server.
4. Connect to the WebCenter Content user interface.
5. Run the following `updateRIDCConnection()` command, on one line, with the appropriate SSL port:

   ```
   updateRIDCConnection('Oracle WebCenter Content - Web UI',
   'WccAdfDefaultConnection',
   connUrl='https://adc2120610.example.com:16201/cs/idcplg',
   credUsername='weblogic',credPassword='password',httpLibrary='oracle',
   credImpersonationAllowed='true')
   ```

Note: In case the `httpLibrary` attribute is not set to `oracle` in the preceding command, Apache 3/4 is used for HTTP or HTTPS communication, so it is necessary to explicitly add the `httpclient/httpcodec` JAR in the WebCenter Content user interface (Model) classpath.

---

6. Restart the WebCenter Content Managed Server.

Over any secured connection, you need to follow the Certificate Authorities required to access secure sites using the SSL protocol. These Certificate Authorities may comprise the Identity and Trusted store.

If you see the following error on the WebCenter Content user interface Managed Server as soon as you try accessing it, you need to import the certificate for Content Server from the Oracle WebCenter Content domain to the WebCenter Content user interface domain:

```
Caused By: javax.net.ssl.SSLHandshakeException:
sun.security.validator.ValidatorException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid
certification path to requested target
```

This error happens because the certificate present in the WebLogic Server trusted store for the WebCenter Content user interface domain does not match or contain the `cacerts` present in the Oracle WebCenter Content domain (which includes Content Server). Therefore, you need to import this certificate and install it in the trusted keystore for the WebCenter Content user interface domain.

To import the certificate from the Oracle WebCenter Content domain to the WebCenter Content user interface domain:

1. Export the Content Server certificate from a browser by opening the Content Server HTTPS URL and saving the certificate as, for example, `contentservercertificate.cer`.
2. Run the keytool utility from the same JDK location that is used by the WebLogic Server trusted keystore. You can find this location in the Administration Console, on the **Keystores** tab for the WebCenter Content user interface Managed Server. For example:

   ```
   JAVA_HOME/bin/java/keytool -import -keystore
   JAVA_HOME/jre/lib/security/cacerts -file contentservercertificate.cer
   ```

   The output from this command is details about the certificate and a request for confirmation.
3. Confirm the certificate:

   ```
   Trust this certificate? [no]: y

   Certificate was added to keystore
   ```

   If you are prompted for a password after running the preceding command, you can specify the common password for a keystore.

12.8.7 Setting Connection Attributes Through Fusion Middleware Control

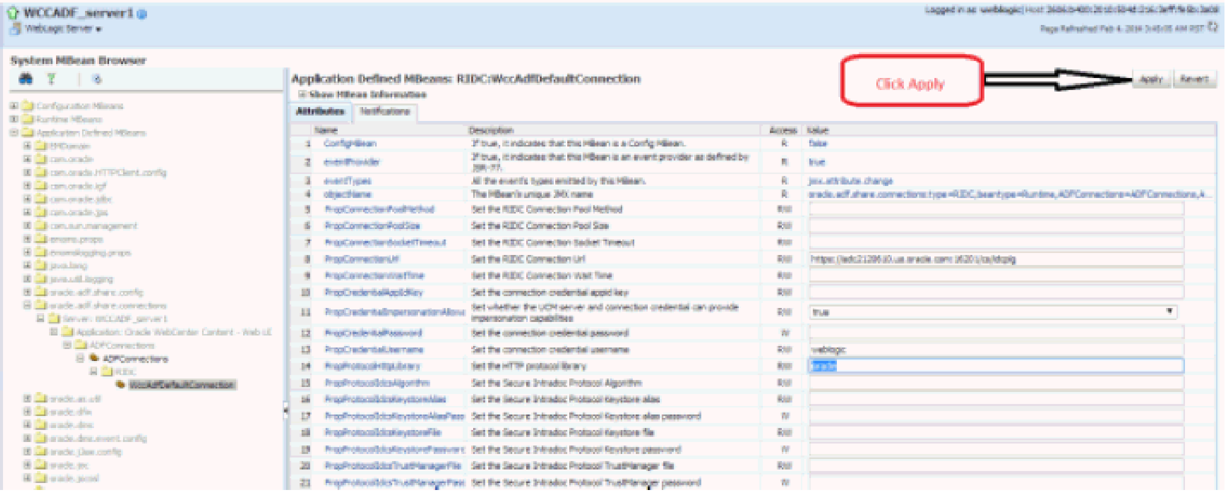
Instead of using the WLST `updateRIDCConnection` command, you can set connection attributes for the WebCenter Content user interface Managed Server through Oracle Enterprise Manager Fusion Middleware Control, in the System MBean Browser.

To set connection attributes through Fusion Middleware Control:

1. Log in to Fusion Middleware Control for the WebCenter Content user interface managed server.
2. In the navigation tree on the left, expand **WebLogic Domain**, then the folder for the WebCenter Content user interface domain, then the cluster name, and then click the name of the Managed Server.
3. From the **WebLogic Domain** drop-down menu at the top of the Managed Server page, choose **System MBean Browser**.
4. In the System MBean Browser navigation tree, expand **Application Defined MBeans**, then **oracle.adf.share.connections**, then **Server: WCCADF_server1**, then **Application: Oracle WebCenter Content – Web UI**, then **ADFConnections**, and then **RIDC**.

   Or you can enter the connection name, `WccAdfDefaultConnection`, in the MBean filtered search.
5. Click **WccAdfDefaultConnection**.
6. On the **Attributes** tab, change the values of the connection attributes to set up the connection, then click the **Apply** button (top right), as Figure 12–1 shows.

Figure 12–1 System MBean Browser



Application Defined MBeans: RIDC:WccAdfDefaultConnection

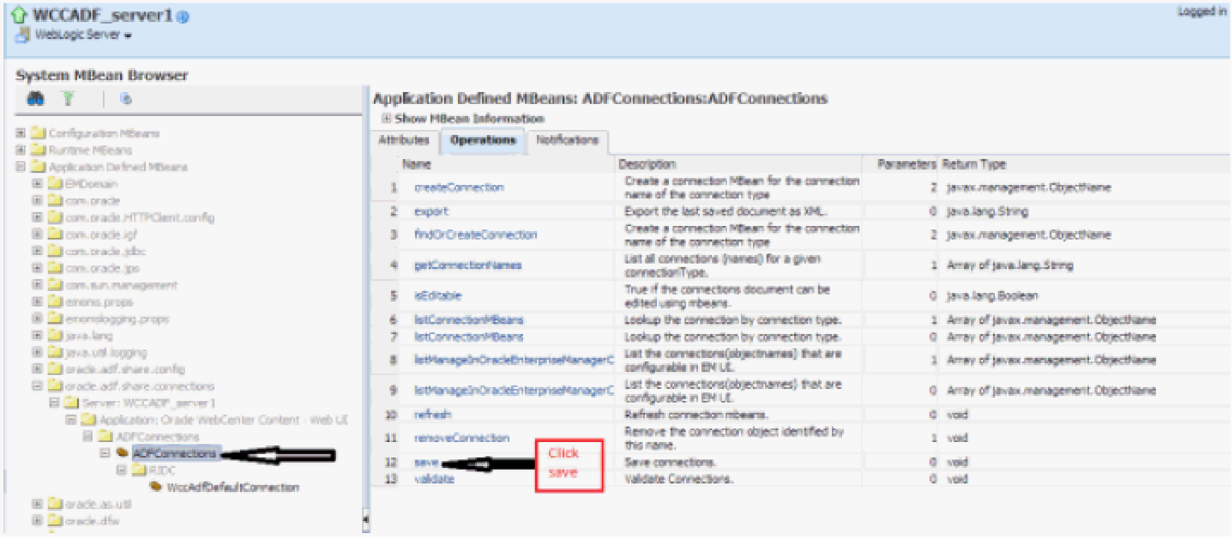
	Name	Description	Access	Value
1	ConfigMBean	If true, it indicates that this MBean is a Config MBean.	R	false
2	eventProvider	If true, it indicates that this MBean is an event provider as defined by JSR-77.	R	true
3	eventTypes	All the event's types emitted by this MBean.	R	jmx.attribute.change
4	objectName	The MBean's unique JMX name	R	oracle.adf.share.connections:type=RIDC,beantype=Runtime,ADFConnections=ADFConnections,A...
5	PropConnectionPoolMethod	Set the RIDC Connection Pool Method	RW	
6	PropConnectionPoolSize	Set the RIDC Connection Pool Size	RW	
7	PropConnectionSocketTimeout	Set the RIDC Connection Socket Timeout	RW	
8	PropConnectionUrl	Set the RIDC Connection Url	RW	https://adc2120610.us.oracle.com:16201/cs/idcplg
9	PropConnectionWaitTime	Set the RIDC Connection Wait Time	RW	
10	PropCredentialAppIdKey	Set the connection credential appid key	RW	
11	PropCredentialsImpersonationAllow	Set whether the UCM server and connection credential can provide impersonation capabilities	RW	true
12	PropCredentialsPassword	Set the connection credential password	W	
13	PropCredentialUsername	Set the connection credential username	RW	weblogic
14	PropProtocolHttpLibrary	Set the HTTP protocol library	RW	oracle
15	PropProtocolIdcsAlgorithm	Set the Secure Intradoc Protocol Algorithm	RW	
16	PropProtocolIdcsKeystoreAlias	Set the Secure Intradoc Protocol Keystore alias	RW	
17	PropProtocolIdcsKeystoreAliasPass	Set the Secure Intradoc Protocol Keystore alias password	W	
18	PropProtocolIdcsKeystoreFile	Set the Secure Intradoc Protocol Keystore file	RW	
19	PropProtocolIdcsKeystorePasswor	Set the Secure Intradoc Protocol Keystore password	W	
20	PropProtocolIdcsTrustManagerFile	Set the Secure Intradoc Protocol TrustManager file	RW	
21	PropProtocolIdcsTrustManagerPass	Set the Secure Intradoc Protocol TrustManager password	W	

Note: If you leave the `PropConnectionSocketTimeout` attribute blank, then the default, `60` seconds, becomes the RIDC Connection Socket Timeout value. This value could be a problem for downloading large files that are being converted to TIFF or PDF documents with the annotations burned in. You can set this attribute to a larger value in case you have large files.

7. Go back to the **ADFConnections** page (**Application Defined MBeans>oracle.adf.share.connections> Server: WCCADF_server1> Application: Oracle WebCenter Content – Web UI> ADFConnections**).

8. On the **Operations** tab, click **Save** to persist the changes made to the connection attributes, as Figure 12–2 shows.

Figure 12–2 ADFConnections MBean



Application Defined MBeans: ADFConnections:ADFConnections

⊞ Show MBean Information

	Name	Description	Parameters	Return Type
1	createConnection	Create a connection MBean for the connection name of the connection type	2	javax.management.ObjectName
2	export	Export the last saved document as XML.	0	java.lang.String
3	findOrCreateConnection	Create a connection MBean for the connection name of the connection type	2	javax.management.ObjectName
4	getConnectionNames	List all connections (names) for a given connectionType.	1	Array of java.lang.String
5	isEditable	True if the connections document can be edited using mbeans.	0	java.lang.Boolean
6	listConnectionMBeans	Lookup the connection by connection type.	1	Array of javax.management.ObjectName
7	listConnectionMBeans	Lookup the connection by connection type.	0	Array of javax.management.ObjectName
8	listManageInOracleEnterpriseManagerC	List the connections(objectnames) that are configurable in EM UI.	1	Array of javax.management.ObjectName
9	listManageInOracleEnterpriseManagerC	List the connections(objectnames) that are configurable in EM UI.	0	Array of javax.management.ObjectName
10	refresh	Refresh connection mbeans.	0	void
11	removeConnection	Remove the connection object identified by this name.	1	void
12	save	Save connections.	0	void
13	validate	Validate Connections.	0	void

9. Restart the WebCenter Content user interface Managed Server.

12.9 Completing the Workflow Configuration

To complete the workflow configuration for the WebCenter Content user interface, you need to restart the Managed Servers and verify the configuration. The UseDatabaseWfInQueue configuration variable enables the WebCenter Content user interface to filter workflows assigned to a user. The EmailNotificationType configuration variable specifies where the links in notification emails point for workflows and subscriptions in different Content Server user interfaces, and its default value is NativeWebUI.

To complete the workflow configuration:

1. Make sure that the *WCC_DOMAIN*/ucm/cs/config/config.cfg file contains the EmailNotificationType variable with either of the following settings:

   - To generate emails with links that point only to the WebCenter Content user interface, set EmailNotificationType=ContentUI in config.cfg.

   - To generate emails with links that point to both the WebCenter Content user interface and the native 11*g* user interface, set EmailNotificationType=ContentUI,NativeWebUI in config.cfg.

2. Restart the Content Server Managed Server, as described in Section 10.3, "Restarting a Managed Server."

3. Click the alert that appears on the Content Server home page after restart: **Click to complete workflow setup**.

   Ensure that Content Server returns a success message: Workflow setup is now complete.

4. Restart the WebCenter Content user interface Managed Server.

For more information about workflows, see "Managing Workflows" in *Managing Oracle WebCenter Content*.

A

Installation Screens for Oracle WebCenter Content

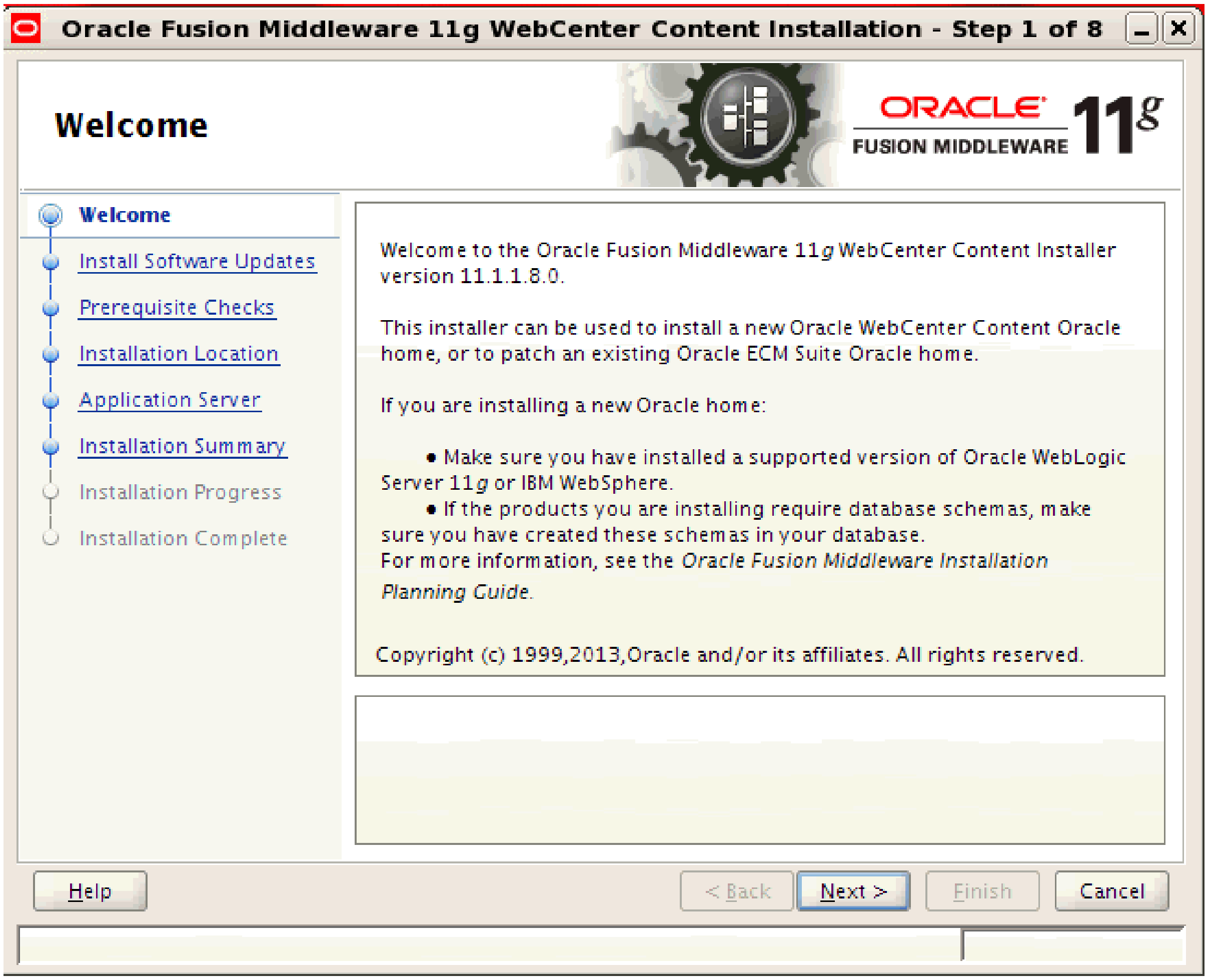
This appendix describes the Oracle Fusion Middleware 11*g* WebCenter Content Installer screens for installing Oracle WebCenter Content.

For information about how to do preinstallation tasks, run the installer, and verify the installation, see Chapter 2, "Installing Oracle WebCenter Content."

This appendix includes the following screens:

- Welcome
- Install Software Updates
- Prerequisite Checks
- Specify Installation Location
- Application Server
- Installation Summary
- Installation Progress
- Installation Complete

A.1 Welcome



Welcome to the Oracle Fusion Middleware 11*g* WebCenter Content Installer version 11.1.1.8.0.

This installer can be used to install a new Oracle WebCenter Content Oracle home, or to patch an existing Oracle ECM Suite Oracle home.

If you are installing a new Oracle home:

- Make sure you have installed a supported version of Oracle WebLogic Server 11*g* or IBM WebSphere.
- If the products you are installing require database schemas, make sure you have created these schemas in your database.

For more information, see the *Oracle Fusion Middleware Installation Planning Guide*.

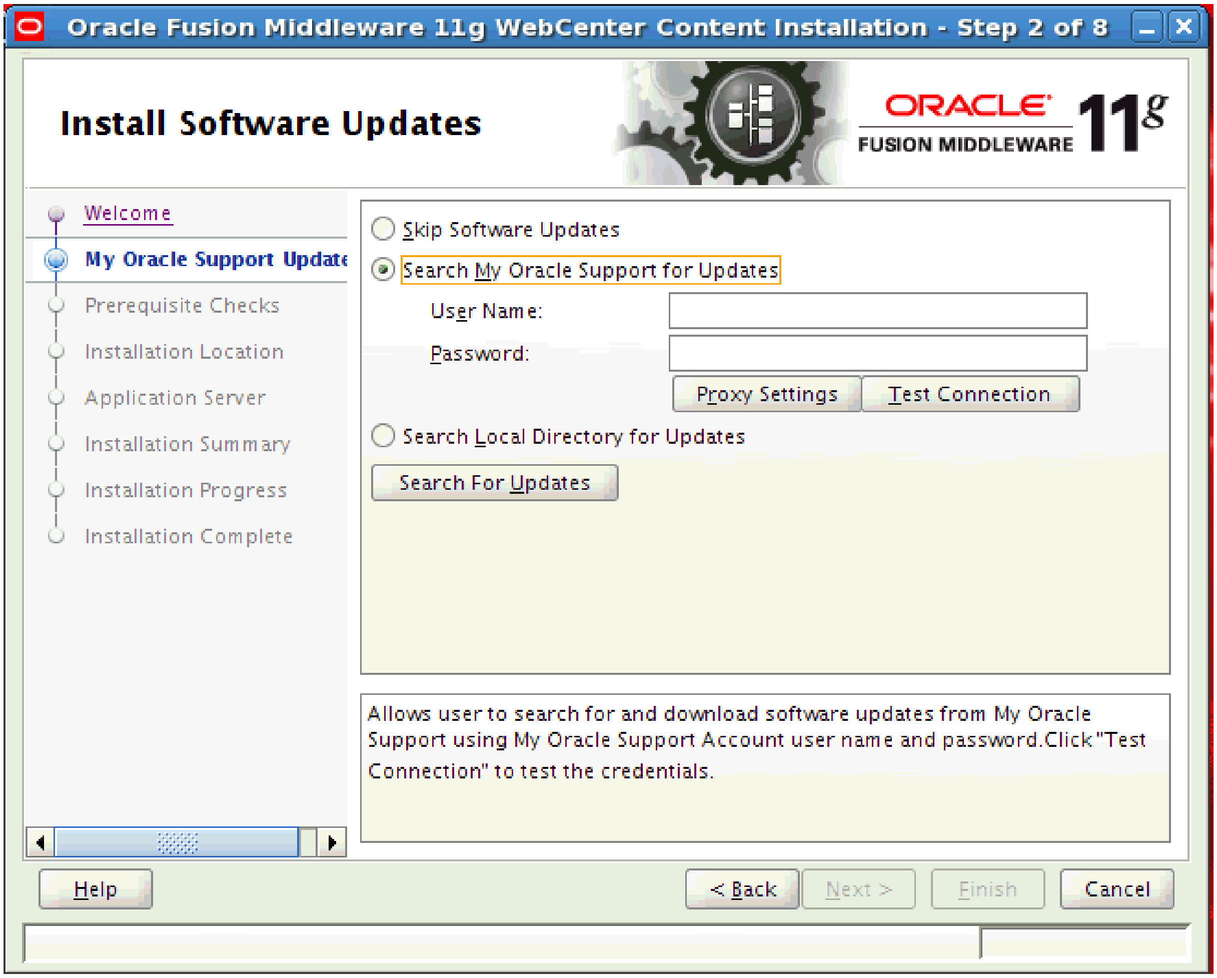
Copyright (c) 1999,2013,Oracle and/or its affiliates. All rights reserved.

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



Oracle Fusion Middleware 11g WebCenter Content Installation - Step 2 of 8

Install Software Updates

○ Skip Software Updates

● Search My Oracle Support for Updates

User Name:

Password:

○ Search Local Directory for Updates

Allows user to search for and download software updates from My Oracle Support using My Oracle Support Account user name and password.Click "Test Connection" to test the credentials.

This screen enables you to search for and install software updates before you install Oracle WebCenter Content. The second link on the left is **My Oracle Support Updates** before you make a selection.

To get updates from My Oracle Support, you can select **Search My Oracle Support for Updates**, specify a user name and password, and then click **Search for Updates**. Before you search, you can click **Proxy Settings** to change the settings for the proxy server and **Test Connection** to test the credentials.

To get updates that you have saved to your computer, you can select **Search Local Directory for Updates**, specify a directory, and then click **Search for Updates**.

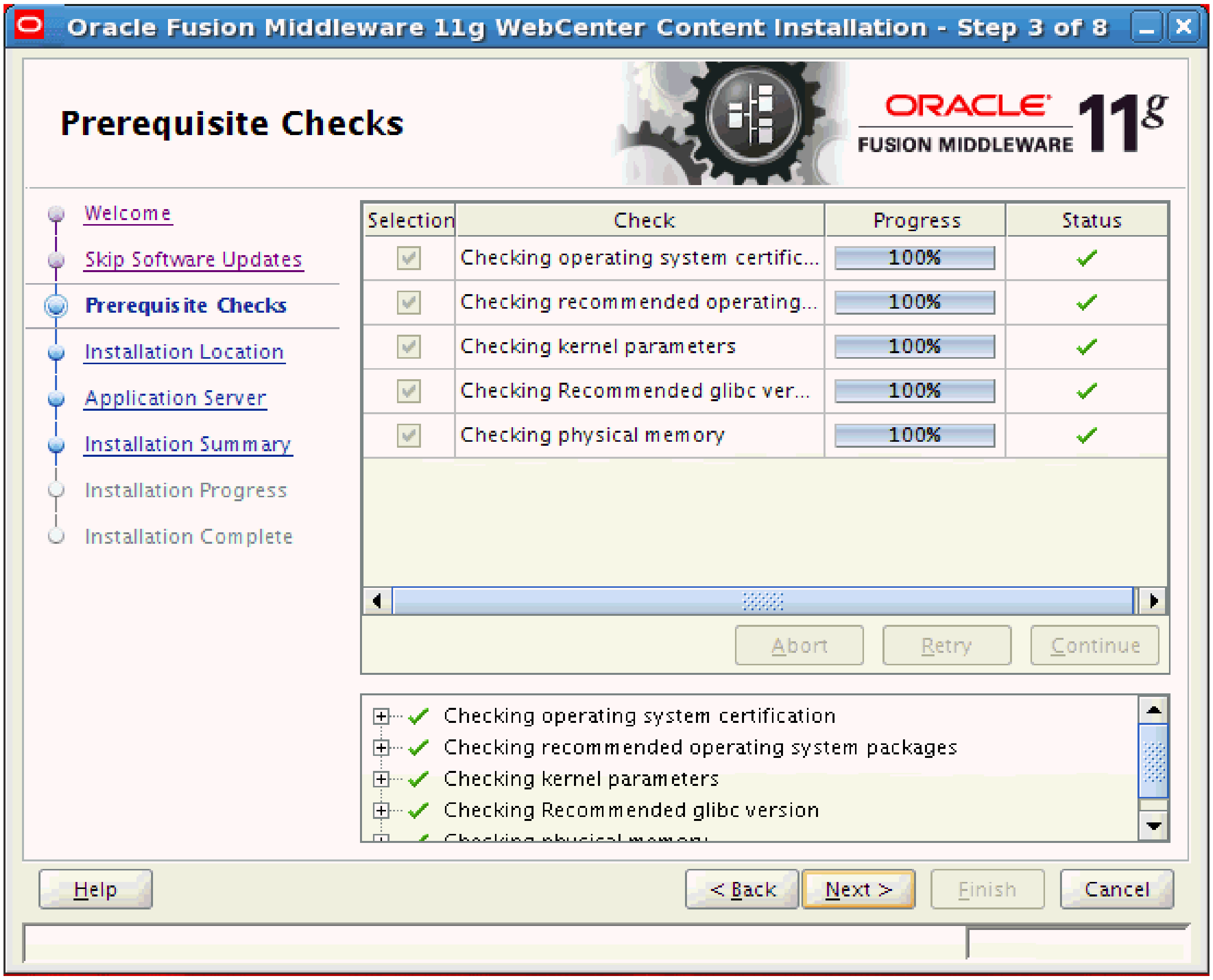
If you do not want to update any software, you can select **Skip Software Updates**. The link on the left changes from **My Oracle Support Updates** to **Skip Software Updates**.

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

The **Next** button starts the software updates or continues the installation.

The **Cancel** button stops the installation.

A.3 Prerequisite Checks



Selection	Check	Progress	Status
☑	Checking operating system certific...	100%	✓
☑	Checking recommended operating...	100%	✓
☑	Checking kernel parameters	100%	✓
☑	Checking Recommended glibc ver...	100%	✓
☑	Checking physical memory	100%	✓

✓ Checking operating system certification
✓ Checking recommended operating system packages
✓ Checking kernel parameters
✓ Checking Recommended glibc version
✓ Checking physical memory

This screen shows the prerequisite checks for a Linux operating system. Only three checks are performed for a Windows operating system:

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

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

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

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

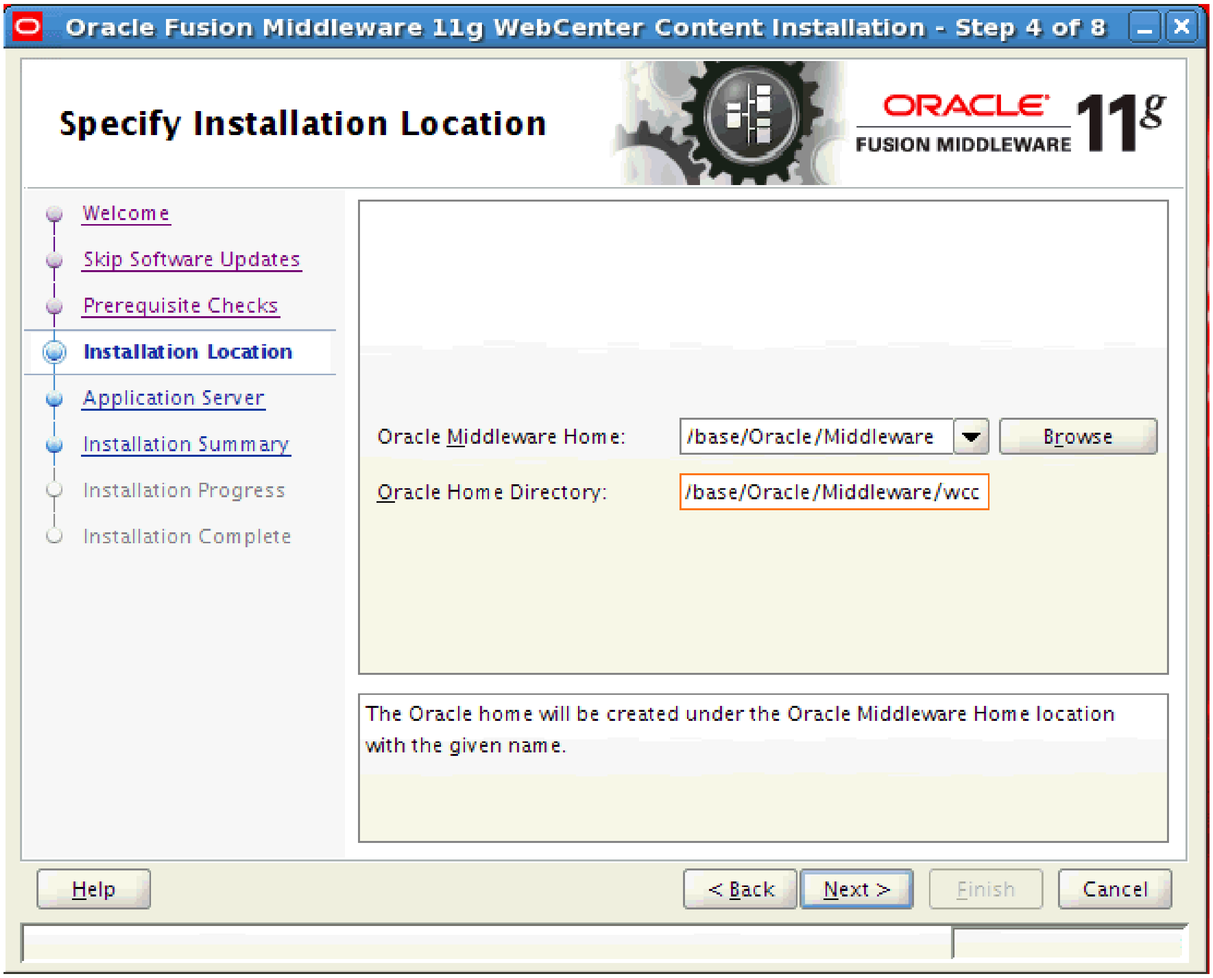
The **Continue** button continues the installation even if the screen displays an error or warning message.

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

The **Next** button continues the installation after the prerequisite checks complete with no errors.

The **Cancel** button stops the installation.

A.4 Specify Installation Location



Oracle Middleware Home: /base/Oracle/Middleware

Oracle Home Directory: /base/Oracle/Middleware/wcc

The Oracle home will be created under the Oracle Middleware Home location with the given name.

The **Oracle Middleware Home** field specifies the absolute path to an existing Middleware home directory. The **Browse** button displays directories that exist on your system.

The **Oracle Home Directory** field specifies a directory in which to install Oracle WebCenter Content (the WebCenter Content Oracle home directory). This directory must be empty. If the directory does not exist, the installer creates it.

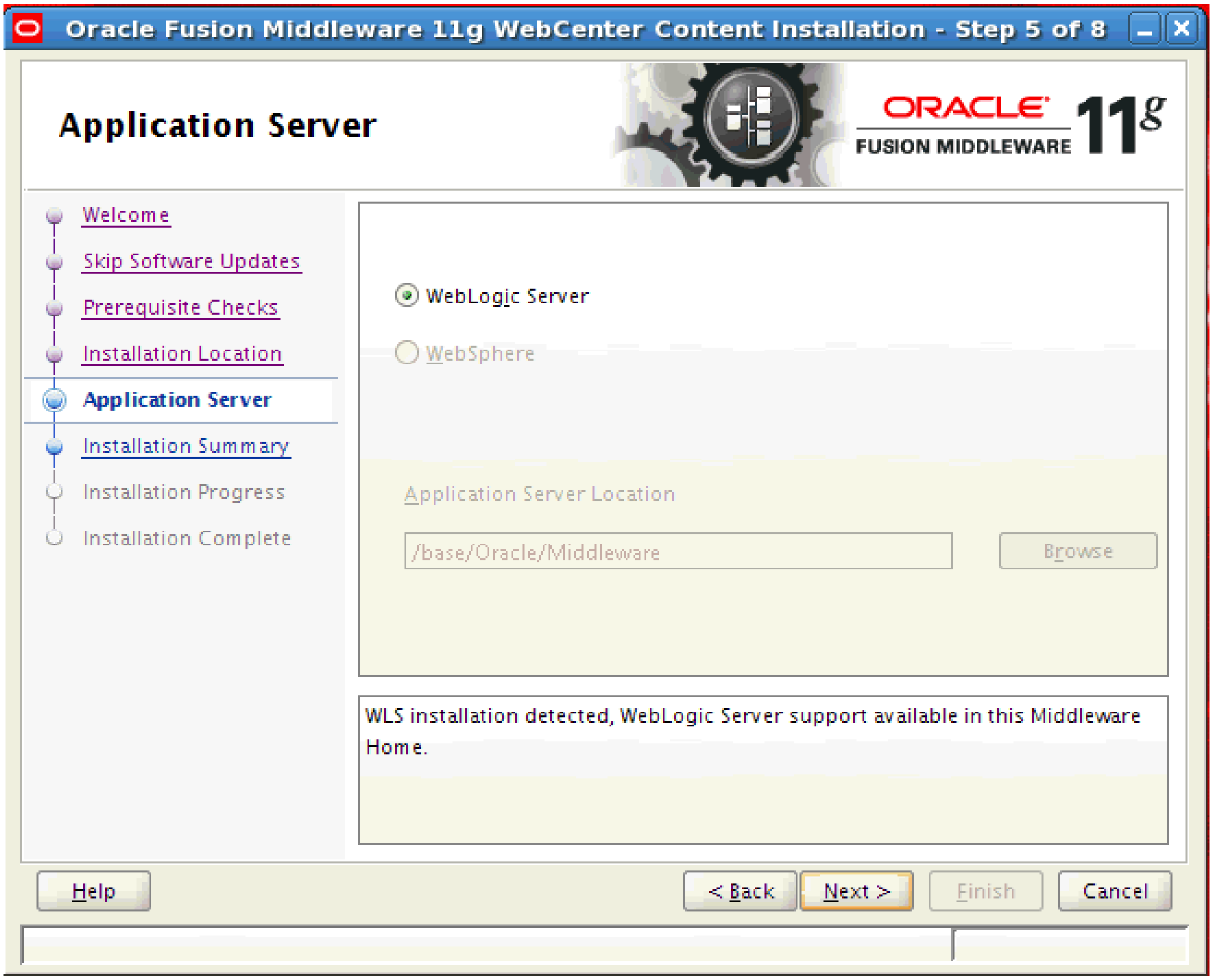
The WebCenter Content Oracle home directory is where all Oracle WebCenter Content products will be installed. All software binaries will reside in this directory, and no runtime process can write to this directory.

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

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

The **Cancel** button stops the installation.

A.5 Application Server



Application Server

● WebLogic Server

○ WebSphere

Application Server Location: /base/Oracle/Middleware

WLS installation detected, WebLogic Server support available in this Middleware Home.

This screen specifies the application server and its location.

The **WebLogic Server** option installs Oracle WebCenter Content on an Oracle WebLogic Server.

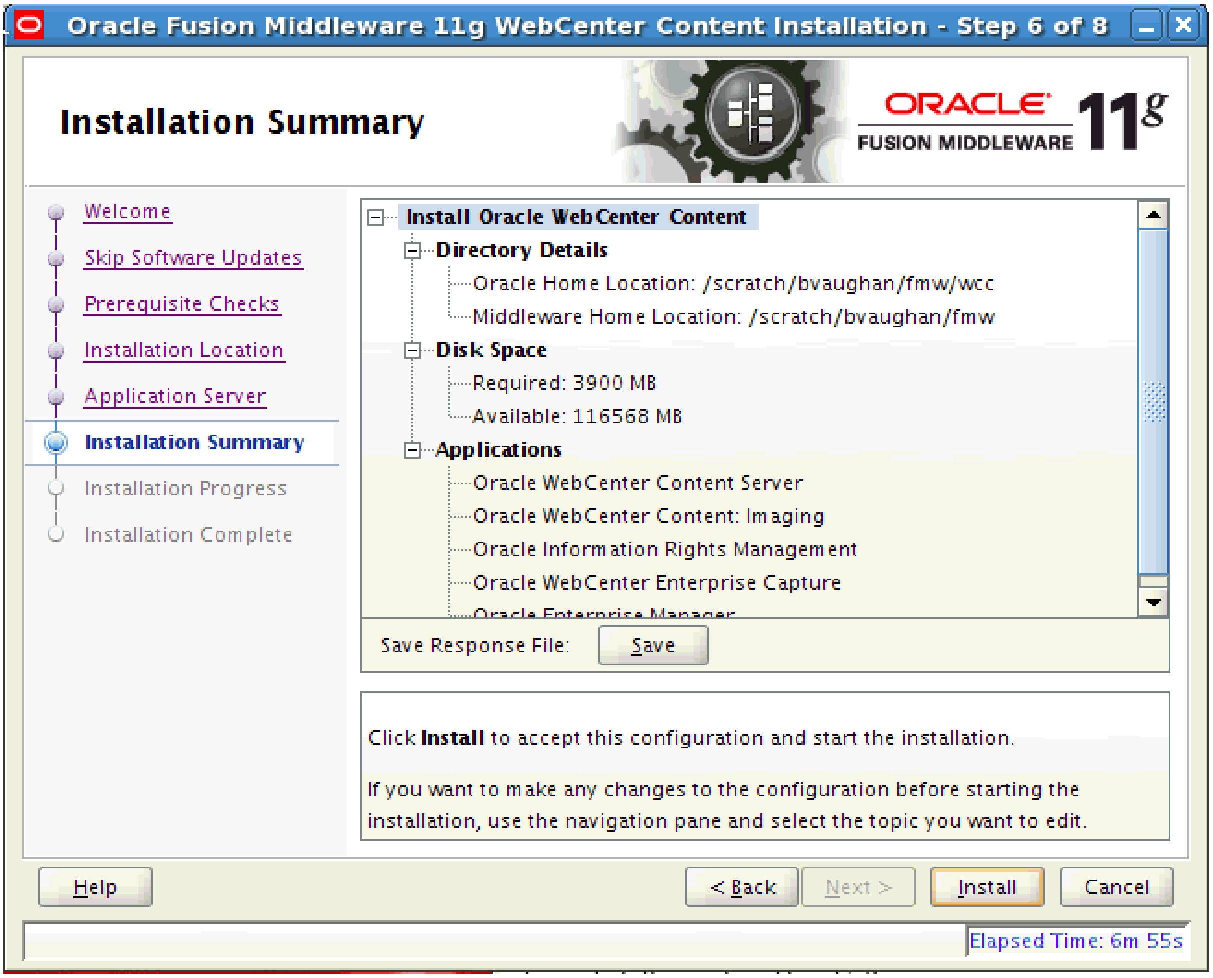
The **WebSphere** option installs Oracle WebCenter Content on an IBM WebSphere Application Server. For more information about a WebSphere installation, see "Installing and Configuring Oracle Fusion Middleware on IBM WebSphere" and "Managing Oracle WebCenter Content on IBM WebSphere Application Servers" in the *Third-Party Application Server Guide*.

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

The **Next** button continues the installation.

The **Cancel** button stops the installation.

A.6 Installation Summary


Oracle Fusion Middleware 11g WebCenter Content Installation - Step 6 of 8

Installation Summary

Install Oracle WebCenter Content
- Directory Details
  - Oracle Home Location: /scratch/bvaughan/fmw/wcc
  - Middleware Home Location: /scratch/bvaughan/fmw
- Disk Space
  - Required: 3900 MB
  - Available: 116568 MB
- Applications
  - Oracle WebCenter Content Server
  - Oracle WebCenter Content: Imaging
  - Oracle Information Rights Management
  - Oracle WebCenter Enterprise Capture
  - Oracle Enterprise Manager

Save Response File: Save

Click **Install** to accept this configuration and start the installation.

If you want to make any changes to the configuration before starting the installation, use the navigation pane and select the topic you want to edit.

This screen summarizes the installation configuration.

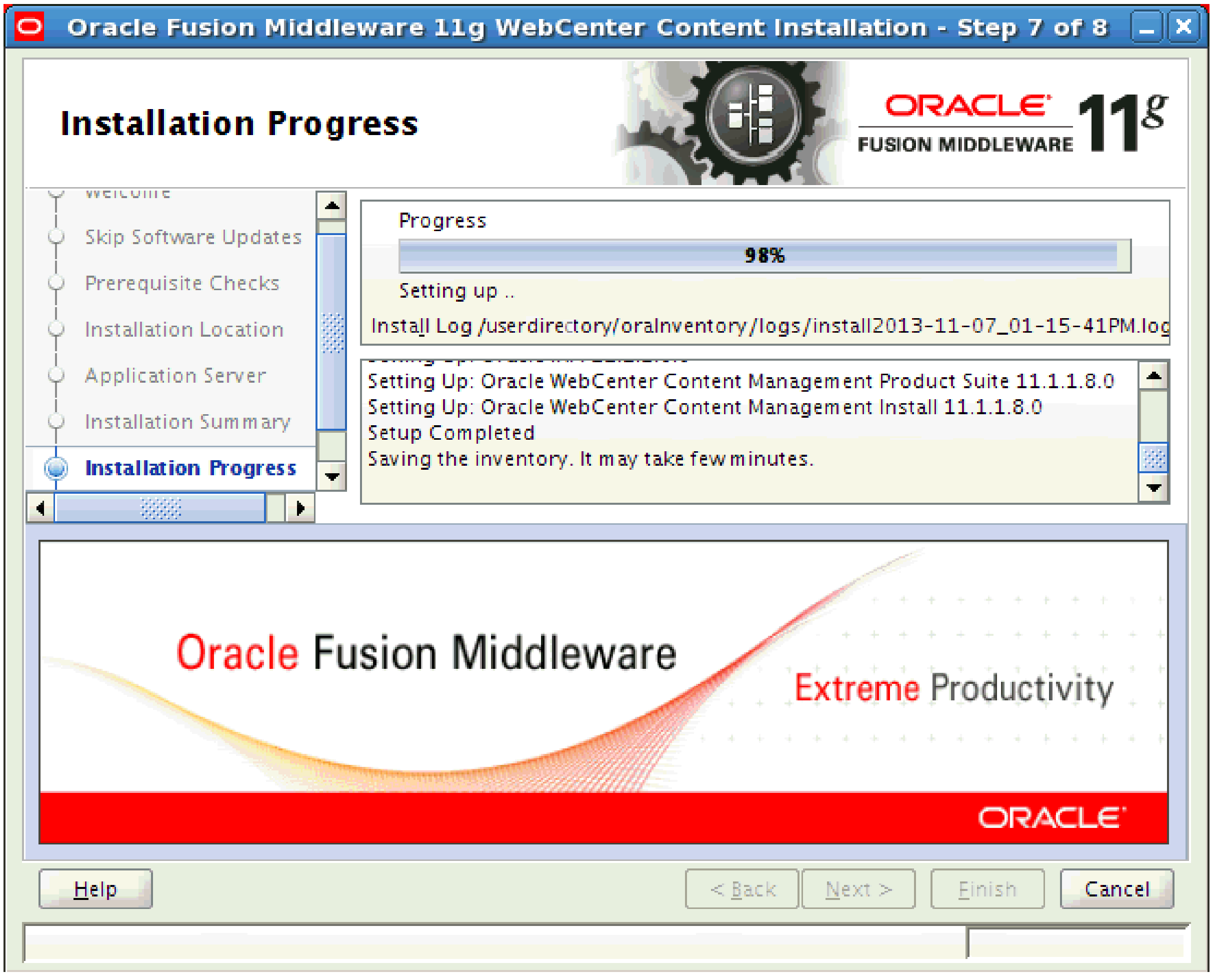
The **Save** button saves the installation configuration in a file, which you can use later to perform the same installation from the command line.

The **Back** button or a link in the navigation tree on the left returns to a previous screen, where you can change the configuration.

The **Install** button begins the installation, with the configuration summarized on this screen.

The **Cancel** button stops the installation.

A.7 Installation Progress



Setting up ..

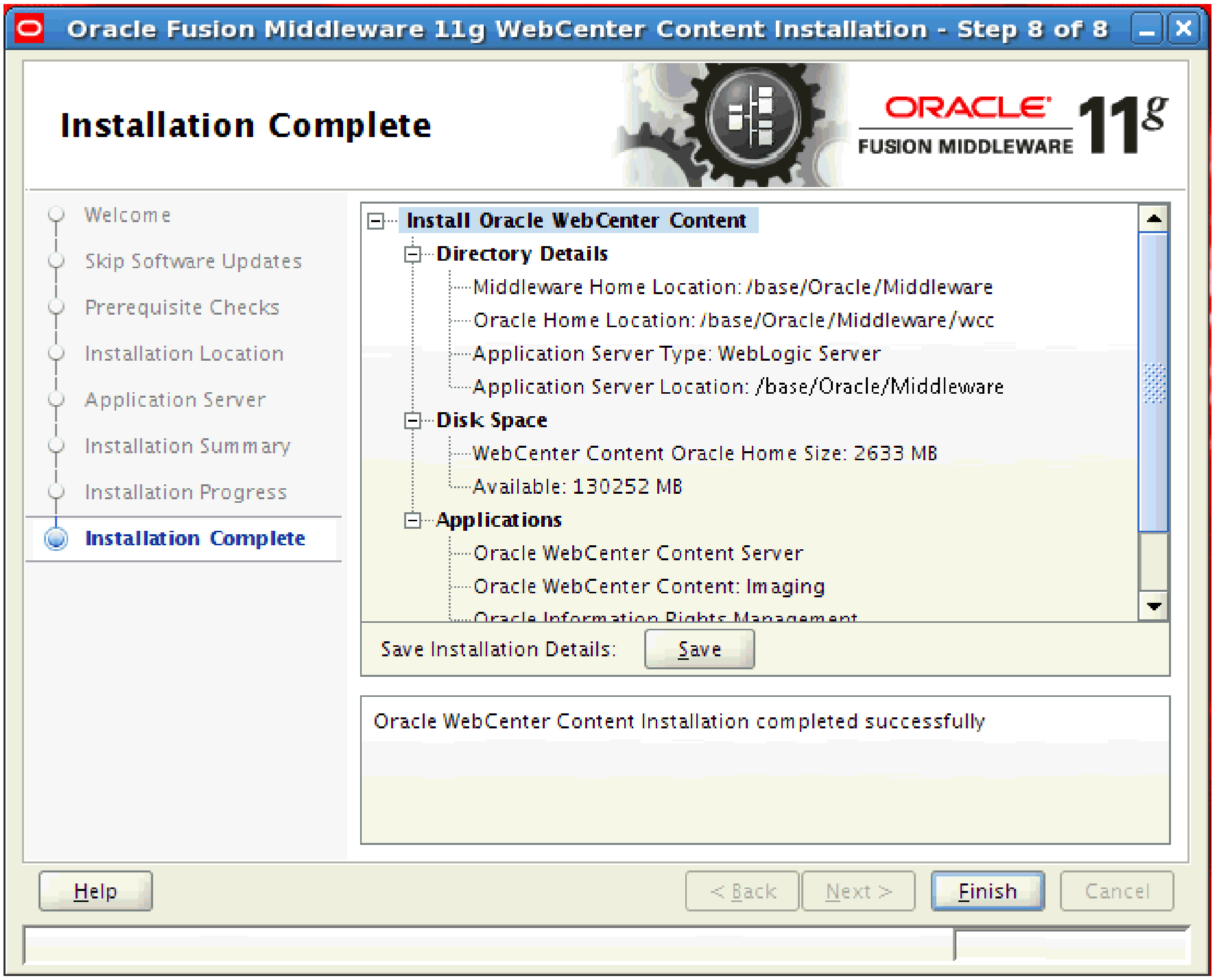
Install Log /userdirectory/oraInventory/logs/install2013-11-07_01-15-41PM.log

```
Setting Up: Oracle WebCenter Content Management Product Suite 11.1.1.8.0
Setting Up: Oracle WebCenter Content Management Install 11.1.1.8.0
Setup Completed
Saving the inventory. It may take few minutes.
```

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

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

A.8 Installation Complete



Install Oracle WebCenter Content
- Directory Details
  - Middleware Home Location: /base/Oracle/Middleware
  - Oracle Home Location: /base/Oracle/Middleware/wcc
  - Application Server Type: WebLogic Server
  - Application Server Location: /base/Oracle/Middleware
- Disk Space
  - WebCenter Content Oracle Home Size: 2633 MB
  - Available: 130252 MB
- Applications
  - Oracle WebCenter Content Server
  - Oracle WebCenter Content: Imaging
  - Oracle Information Rights Management

Save Installation Details:

Oracle WebCenter Content Installation completed successfully

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

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

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

B

Configuration Screens for Oracle WebCenter Content

This appendix describes some Fusion Middleware Configuration Wizard screens for configuring Oracle WebCenter Content applications in an Oracle WebLogic Server domain.

For information about how to run the Configuration Wizard and do initial configuration tasks, see Chapter 3, "Configuring Oracle WebCenter Content Applications." For additional information about configuring individual Oracle WebCenter Content products, see these chapters:

- Chapter 4, "Completing the WebCenter Content Configuration"
- Chapter 5, "Completing the Inbound Refinery Configuration"
- Chapter 6, "Completing the Imaging Configuration"
- Chapter 7, "Completing the Oracle WebCenter Enterprise Capture Configuration"
- Chapter 8, "Completing the Records Configuration"
- Chapter 9, "Completing the Oracle IRM Configuration"

For information about how to verify the configuration, see Chapter 10, "Verifying the Oracle WebCenter Content Configuration."

For more information about the screens in this appendix and other configuration screens, see "Configuration Wizard Screens" in *Creating Domains Using the Configuration Wizard*.

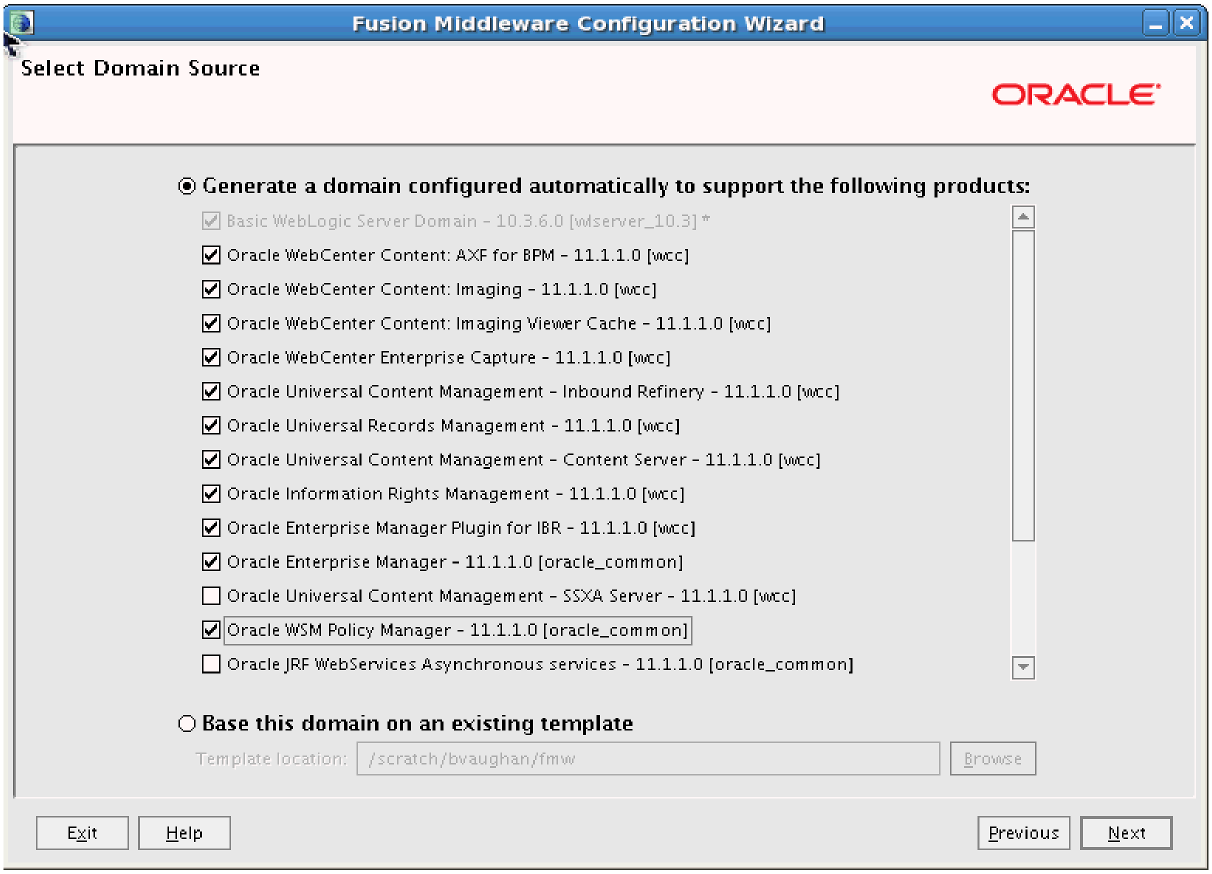
This appendix includes the following screens:

- Select Domain Source
- Select Extension Source
- Configure JDBC Component Schema
- Select Optional Configuration
- Select JMS Distributed Destination Type
- Configure Managed Servers
- Configure Clusters
- Assign Servers to Clusters
- Configure Machines
- Assign Servers to Machines

- Target Deployments to Clusters or Servers
- Target Services to Clusters or Servers

For more information about a screen, click the **Help** button on the screen. For more information about configuring Oracle WebLogic Server domains, see *Creating Domains Using the Configuration Wizard*.

B.1 Select Domain Source



Select Domain Source

● Generate a domain configured automatically to support the following products:

☑ Basic WebLogic Server Domain - 10.3.6.0 [wlserver_10.3] *
☑ Oracle WebCenter Content: AXF for BPM - 11.1.1.0 [wcc]
☑ Oracle WebCenter Content: Imaging - 11.1.1.0 [wcc]
☑ Oracle WebCenter Content: Imaging Viewer Cache - 11.1.1.0 [wcc]
☑ Oracle WebCenter Enterprise Capture - 11.1.1.0 [wcc]
☑ Oracle Universal Content Management - Inbound Refinery - 11.1.1.0 [wcc]
☑ Oracle Universal Records Management - 11.1.1.0 [wcc]
☑ Oracle Universal Content Management - Content Server - 11.1.1.0 [wcc]
☑ Oracle Information Rights Management - 11.1.1.0 [wcc]
☑ Oracle Enterprise Manager Plugin for IBR - 11.1.1.0 [wcc]
☑ Oracle Enterprise Manager - 11.1.1.0 [oracle_common]
□ Oracle Universal Content Management - SSXA Server - 11.1.1.0 [wcc]
☑ Oracle WSM Policy Manager - 11.1.1.0 [oracle_common]
□ Oracle JRF WebServices Asynchronous services - 11.1.1.0 [oracle_common]

○ Base this domain on an existing template

Template location: /scratch/bvaughan/fmw

Select **Generate a domain configured automatically to support the following products**, and then select one or more of these product templates:

- **Oracle WebCenter Content: AXF for BPM**
- **Oracle WebCenter Content: Imaging**
- **Oracle WebCenter Enterprise Capture**
- **Oracle Universal Records Management**

  (for Oracle WebCenter Content: Records)
- **Oracle Universal Content Management - Inbound Refinery**

  (for Oracle WebCenter Content: Inbound Refinery)
- **Oracle Universal Content Management - Content Server**

  (for Oracle WebCenter Content)
- **Oracle Information Rights Management**

When you select **Oracle WebCenter Content: Imaging**, you also need to select **Oracle WebCenter Content - Content Server**.

Imaging includes AXF for BPEL. If you are going to use AXF for BPM with Imaging, you need to select Oracle WebCenter Content: AXF for BPM as well as the following product templates:

- **Oracle BPM Suite**
- **Oracle SOA Suite**
- **Oracle WebCenter Content: AXF for BPM**
- **Oracle WebCenter Content: Imaging Viewer Cache**
- **Oracle WebCenter Content: Imaging**
- **Oracle Universal Content Management - Content Server**
- **Oracle Enterprise Manager**
- **Oracle WSM Policy Manager**
- **Oracle JRF**

If you are going to use AXF for BPM or AXF for BPEL with Imaging, and Oracle SOA Suite is deployed to a different domain or installed on a different machine, you will need to run `WCC_ORACLE_HOME\common\config.cmd` on the Oracle SOA Suite machine and select Oracle WebCenter Content: AXF for BPM as well as the following product templates:

- **Oracle SOA Suite**
- **Oracle WSM Policy Manage**r
- **Oracle Enterprise Manager**

When you select **Oracle WebCenter Content: Imaging** on the Select Domain Source screen, **Oracle WebCenter Content: Imaging Viewer Cache** is automatically selected.

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

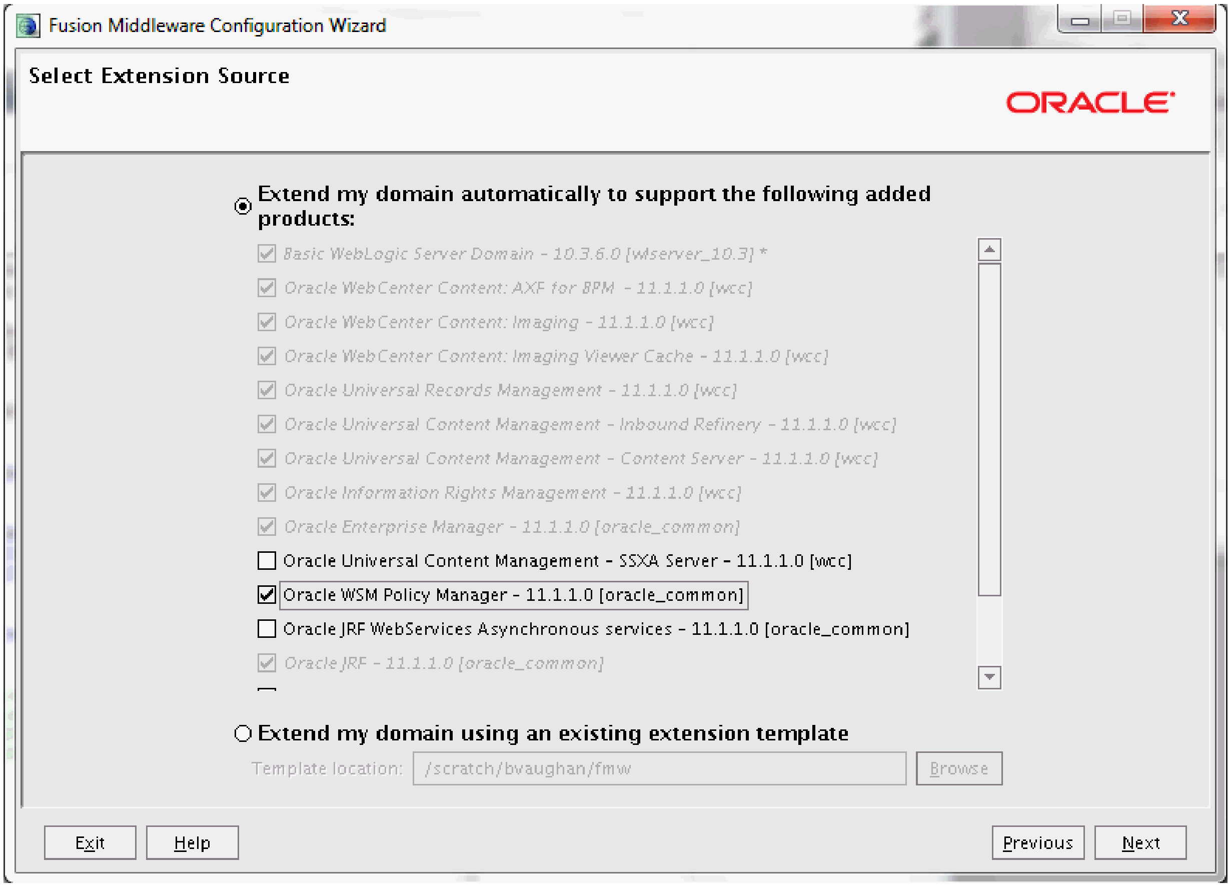
If you want a remote deployment of a Site Studio for External Applications website, you can select **Oracle Universal Content Management - SSXA Server** (for Oracle WebCenter Content - SSXA Server) to create an Oracle WebLogic Server domain with a Managed Server that has the files required to run the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

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

Alternatively, you can select **Base this domain on an existing template** and then click **Browse** to navigate your directories to find an existing template. For more information, see "Select Domain Source" in *Creating Domains Using the Configuration Wizard*.

Click **Next** to continue.

B.2 Select Extension Source



Select Extension Source

● Extend my domain automatically to support the following added products:

☑ Basic WebLogic Server Domain - 10.3.6.0 [wlserver_10.3] *
☑ Oracle WebCenter Content: AXF for BPM - 11.1.1.0 [wcc]
☑ Oracle WebCenter Content: Imaging - 11.1.1.0 [wcc]
☑ Oracle WebCenter Content: Imaging Viewer Cache - 11.1.1.0 [wcc]
☑ Oracle Universal Records Management - 11.1.1.0 [wcc]
☑ Oracle Universal Content Management - Inbound Refinery - 11.1.1.0 [wcc]
☑ Oracle Universal Content Management - Content Server - 11.1.1.0 [wcc]
☑ Oracle Information Rights Management - 11.1.1.0 [wcc]
☑ Oracle Enterprise Manager - 11.1.1.0 [oracle_common]
□ Oracle Universal Content Management - SSXA Server - 11.1.1.0 [wcc]
☑ Oracle WSM Policy Manager - 11.1.1.0 [oracle_common]
□ Oracle JRF WebServices Asynchronous services - 11.1.1.0 [oracle_common]
☑ Oracle JRF - 11.1.1.0 [oracle_common]

○ Extend my domain using an existing extension template

Template location: /scratch/bvaughan/fmw

Select the source from which to extend an existing Oracle WebLogic Server domain. Select **Extend my domain automatically to support the following added products**, and then select one or more of the templates that are not already selected.

- **Oracle WebCenter Content: AXF for BPM**
- **Oracle WebCenter Content: Imaging**
- **Oracle WebCenter Enterprise Capture**
- **Oracle Universal Records Management**

  (for Oracle WebCenter Content: Records)
- **Oracle Universal Content Management - Inbound Refinery**

  (for Oracle WebCenter Content: Inbound Refinery)
- **Oracle Universal Content Management - Content Server**

  (for Oracle WebCenter Content)
- **Oracle Information Rights Management**

When you select **Oracle WebCenter Content: Imaging**, you also need to select **Oracle WebCenter Content - Content Server** if WebCenter Content is not already configured in the domain.

Imaging includes AXF for BPEL. If you are going to use AXF for BPM with Imaging, you need to select Oracle WebCenter Content: AXF for BPM as well as the following product templates (some of these are automatically selected):

- **Oracle BPM Suite**
- **Oracle SOA Suite**
- **Oracle WebCenter Content: AXF for BPM**
- **Oracle WebCenter Content: Imaging Viewer Cache**
- **Oracle WebCenter Content: Imaging**
- **Oracle Universal Content Management - Content Server**
- **Oracle Enterprise Manager**
- **Oracle WSM Policy Manager**
- **Oracle JRF**

If you are going to use AXF for BPM or AXF for BPEL with Imaging, and Oracle SOA Suite is deployed to a different domain or installed on a different machine, you will need to run `WCC_ORACLE_HOME\common\config.cmd` on the Oracle SOA Suite machine and select the following product templates:

- **Oracle SOA Suite**
- **Oracle WSM Policy Manage**r
- **Oracle Enterprise Manager**

When you select **Oracle WebCenter Content: Imaging** on the Select Extension Source screen, **Oracle WebCenter Content: Imaging Viewer Cache** is automatically selected.

When you select any Oracle WebCenter Content application, **Oracle Enterprise Manager** and **Oracle JRF** are automatically selected. If you deselect any of these items that are automatically selected, the Oracle WebCenter Content application will also be deselected.

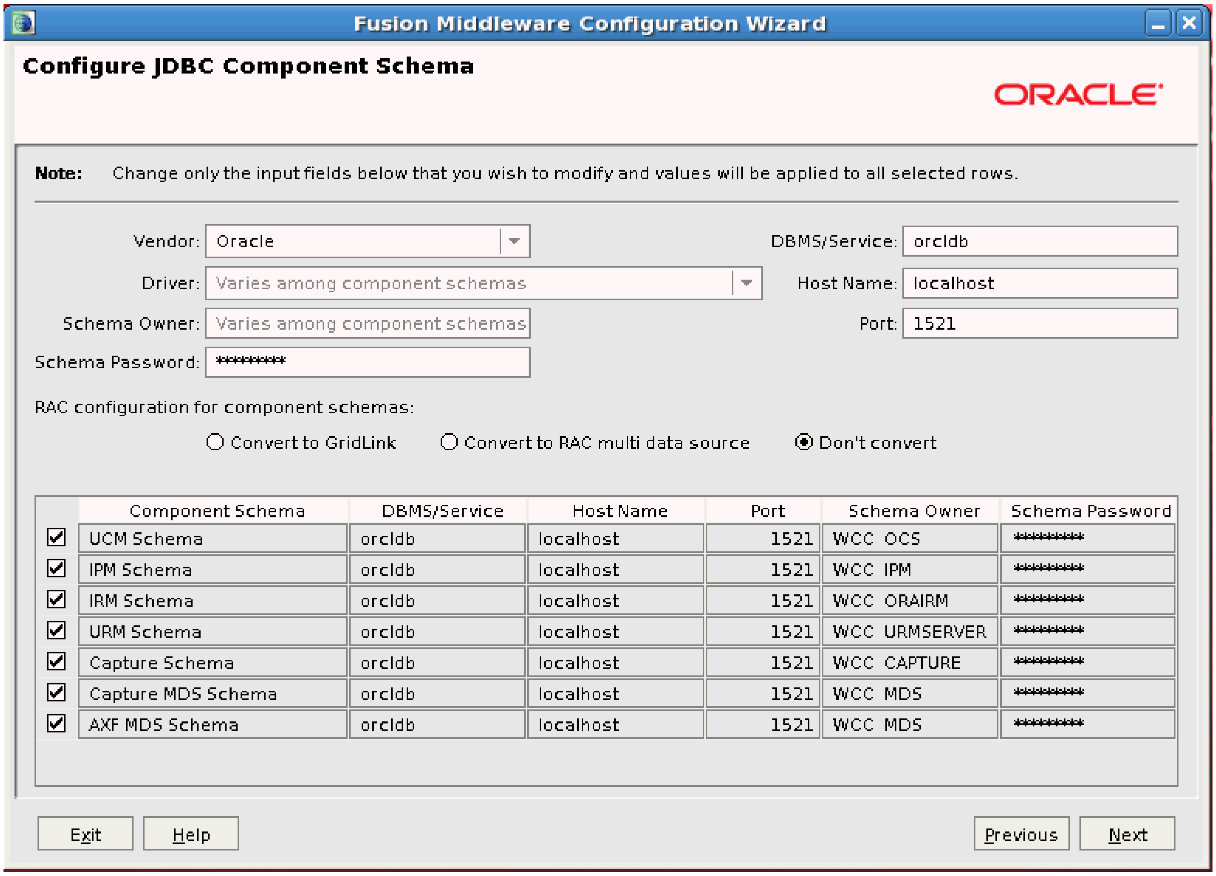
If you want a remote deployment for a Site Studio for External Applications website, you can select **Oracle Universal Content Management - SSXA Server** (for Oracle WebCenter Content - SSXA Server) to extend an Oracle WebLogic Server domain with a Managed Server that has the files required to run the website.

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

Alternatively, you can select **Extend my domain using an existing extension template** and specify the path to the extension template in the **Template location** field. For more information, see "Extend Domain Source" in *Creating Domains Using the Configuration Wizard*.

Click **Next** to continue.

B.3 Configure JDBC Component Schema



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:	Oracle	DBMS/Service:	orcldb
Driver:	Varies among component schemas	Host Name:	localhost
Schema Owner:	Varies among component schemas	Port:	1521
Schema Password:	*********		

RAC configuration for component schemas:

○ Convert to GridLink ○ Convert to RAC multi data source ● Don't convert

	Component Schema	DBMS/Service	Host Name	Port	Schema Owner	Schema Password
☑	UCM Schema	orcldb	localhost	1521	WCC_OCS	*********
☑	IPM Schema	orcldb	localhost	1521	WCC_IPM	*********
☑	IRM Schema	orcldb	localhost	1521	WCC_ORAIRM	*********
☑	URM Schema	orcldb	localhost	1521	WCC_URMSERVER	*********
☑	Capture Schema	orcldb	localhost	1521	WCC_CAPTURE	*********
☑	Capture MDS Schema	orcldb	localhost	1521	WCC_MDS	*********
☑	AXF MDS Schema	orcldb	localhost	1521	WCC_MDS	*********

Use this screen to edit the configuration information for each JDBC component schema. Configure each component schema, including the Oracle WSM MDS schema if it was created with Repository Creation Utility (RCU), by selecting a schema checkbox and then completing the following fields:

- **Component Schema:** Select a component schema row.
- **Vendor:** Select a database vendor from the list.
- **Driver:** Leave the default driver for the database vendor selected, or select a driver for the component schema from the list.
- **Schema Owner:** Enter the user name of the application schema owner, specified during schema creation with RCU.
- **Schema Password:** Enter the schema password, specified during schema creation with RCU.
- **DBMS/Service:** Enter the name of the database instance if `Oracle's Driver (Thin) for Instance connections` is selected in the **Driver** field, or enter the service name (global database name) if `Oracle's Driver (Thin) for Service connections` is selected in the **Driver** field. For Microsoft SQL Server or IBM DB2, you must enter a database name because there is no service name.

  Specify the database that contains the application schema or schemas.

For IBM DB2, if the name of the schema suffix displayed on the screen is longer than 3 characters, you need to change it to the name specified for the schema when it was created in the Repository Creation Utility (see Section 2.2.2, "Creating Schemas for Oracle WebCenter Content Applications"). For example, change `DEV_CAPTURE` to `DEV_ODC`, `DEV_URMSERVER` to `DEV_URM`, and `DEV_ORAIRM` to `DEV_IRM`.

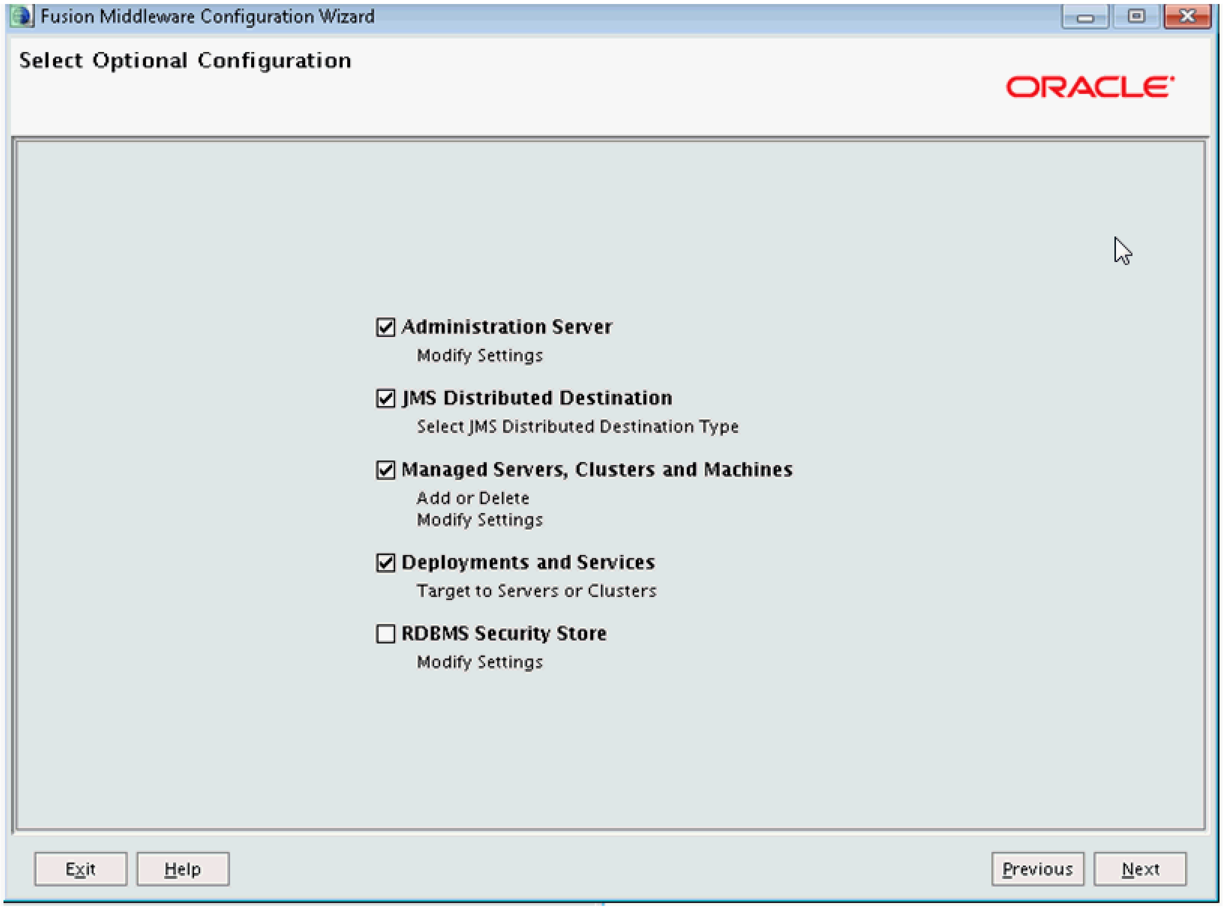
For Oracle RAC databases, specify the service name of one of the nodes in this field. For example: `sales.example.com`.

- **Host Name:** Specify the name of the machine on which your database resides, in the format `host.example.com`. For Oracle RAC databases, specify the Virtual IP name or one of the node names as the host name.
- **Listen Port:** Specify the database listen port number. The default port number is 1521 for an Oracle Database instance, `1433` for Microsoft SQL Server, or `50000` for IBM DB2.

Click **Next** to continue.

For more information, see "Configure JDBC Component Schema" in *Creating Domains Using the Configuration Wizard*.

B.4 Select Optional Configuration



Fusion Middleware Configuration Wizard

Select Optional Configuration

☑ Administration Server
Modify Settings

☑ JMS Distributed Destination
Select JMS Distributed Destination Type

☑ Managed Servers, Clusters and Machines
Add or Delete
Modify Settings

☑ Deployments and Services
Target to Servers or Clusters

☐ RDBMS Security Store
Modify Settings

Optionally, select any or all of these options for configuring the Administration Server and Managed Servers:

- **Administration Server**
- **JMS Distributed Destination**
- **Managed Servers, Clusters and Machines**
- **Deployments and Services**
- **RDBMS Security Store**

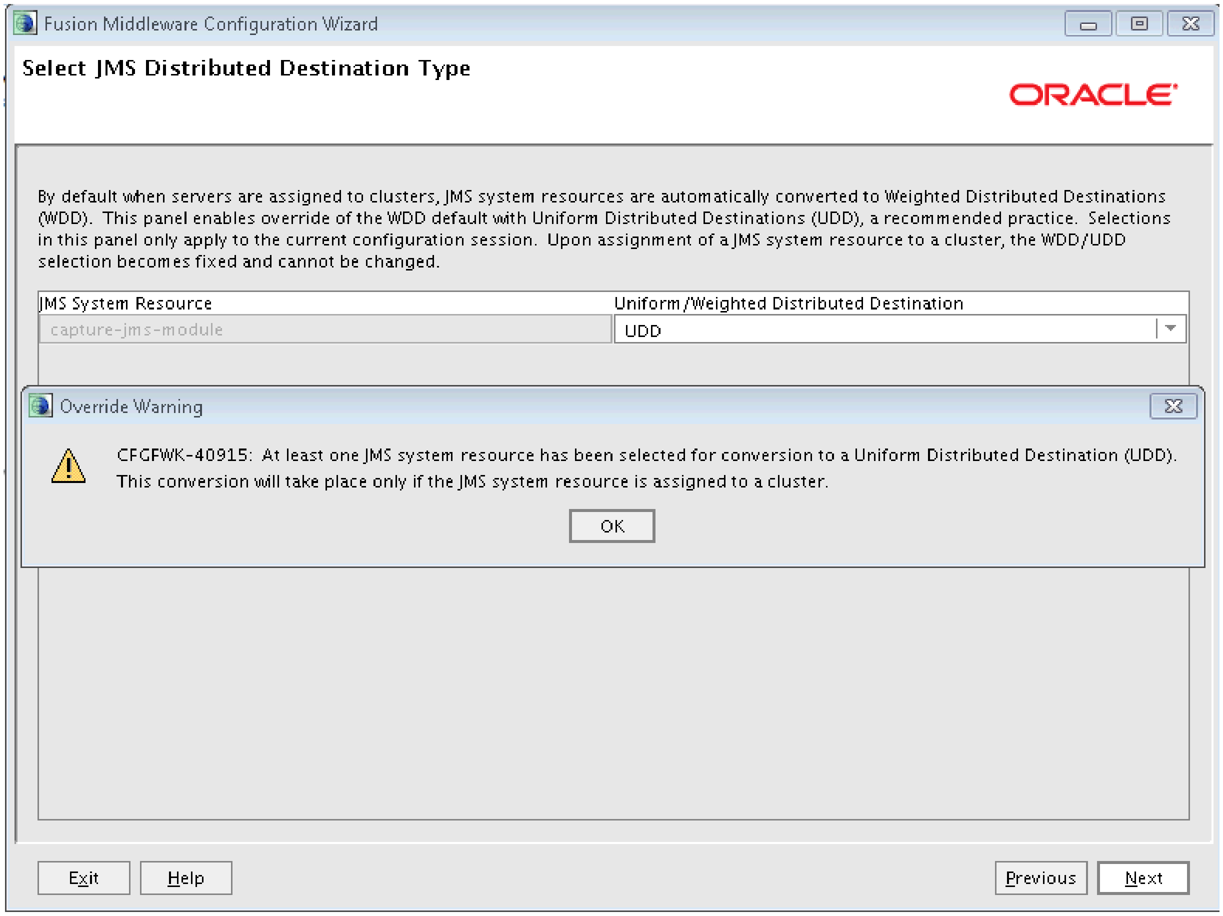
Select one or more of these options if you want to change any default settings. For example, select **Administration Server** to configure SSL for it or change its port number, or select **Managed Servers, Clusters and Machines** to change the name or port for a Managed Server, add it to a cluster, or configure a machine for it.

For Oracle IRM, you should select **Administration Server**, **Managed Servers, Clusters and Machines**, and **Deployments and Services**.

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

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.

B.5 Select JMS Distributed Destination Type


Fusion Middleware Configuration Wizard
Select JMS Distributed Destination Type
ORACLE

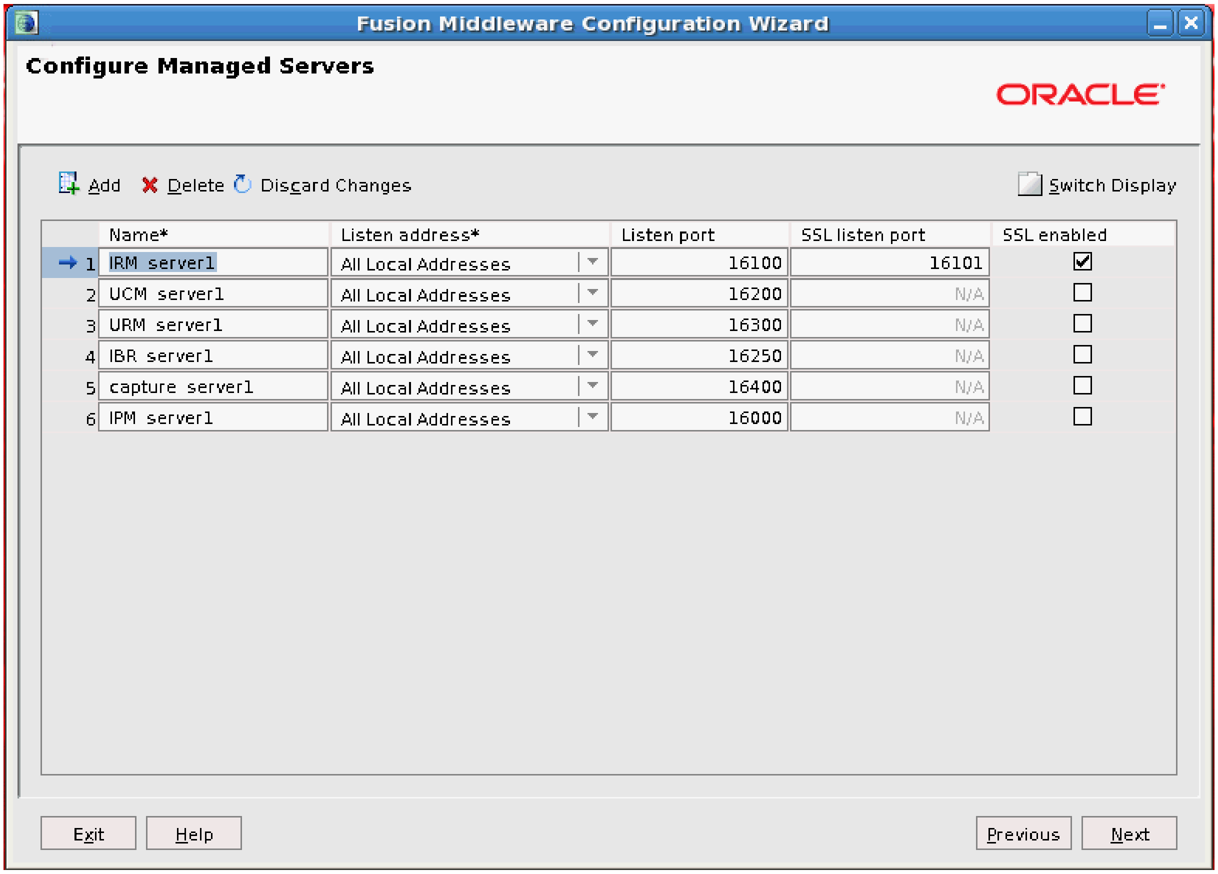
By default when servers are assigned to clusters, JMS system resources are automatically converted to Weighted Distributed Destinations (WDD). This panel enables override of the WDD default with Uniform Distributed Destinations (UDD), a recommended practice. Selections in this panel only apply to the current configuration session. Upon assignment of a JMS system resource to a cluster, the WDD/UDD selection becomes fixed and cannot be changed.

JMS System Resource	Uniform/Weighted Distributed Destination
capture-jms-module	UDD

CFGFWK-40915: At least one JMS system resource has been selected for conversion to a Uniform Distributed Destination (UDD). This conversion will take place only if the JMS system resource is assigned to a cluster.

Accept the default (UDD), and click **Next**. Click **OK** in the override warning.

B.6 Configure Managed Servers



	Name*	Listen address*	Listen port	SSL listen port	SSL enabled
1	IRM server1	All Local Addresses	16100	16101	☑
2	UCM server1	All Local Addresses	16200	N/A	□
3	URM server1	All Local Addresses	16300	N/A	□
4	IBR server1	All Local Addresses	16250	N/A	□
5	capture server1	All Local Addresses	16400	N/A	□
6	IPM server1	All Local Addresses	16000	N/A	□

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**

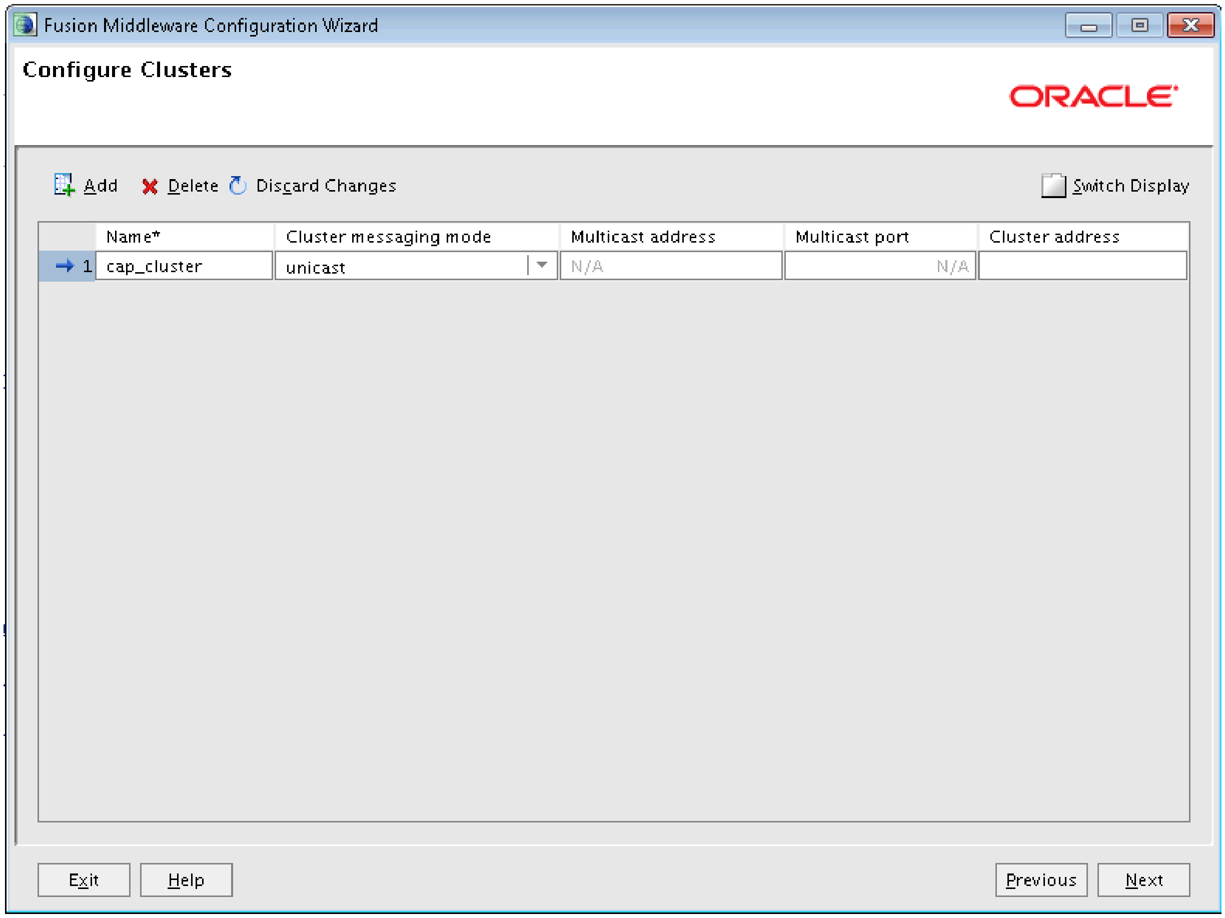
  Port number for SSL connections, active when **SSL enabled** is selected in the same row

- **SSL Enabled**

  Enabled if selected and if a port number for SSL connections is provided in the same row

Click **Next** to continue.

B.7 Configure Clusters



	Name*	Cluster messaging mode	Multicast address	Multicast port	Cluster address
1	cap_cluster	unicast	N/A	N/A	

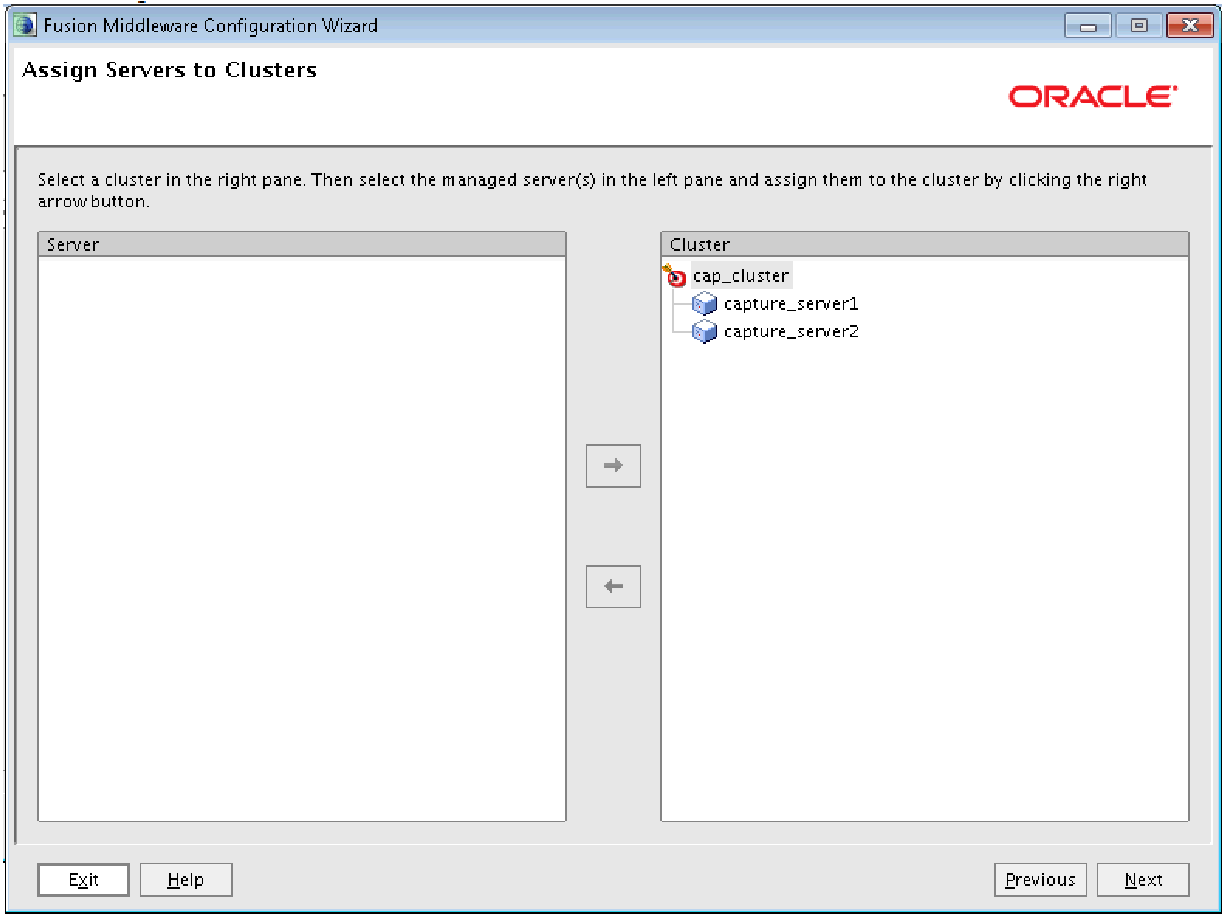
Optionally, configure one or more clusters. For example, for a Capture cluster of two Managed Servers, create a cluster named `cap_cluster` with the **Cluster messaging mode** value `unicast`.

Notes:

- To use clusters, you need a license for Oracle WebLogic Server Enterprise Edition.
- If you decide to configure a cluster, then you must assign a cluster address.

Click **Next** to continue.

B.8 Assign Servers to Clusters



Assign Servers to Clusters

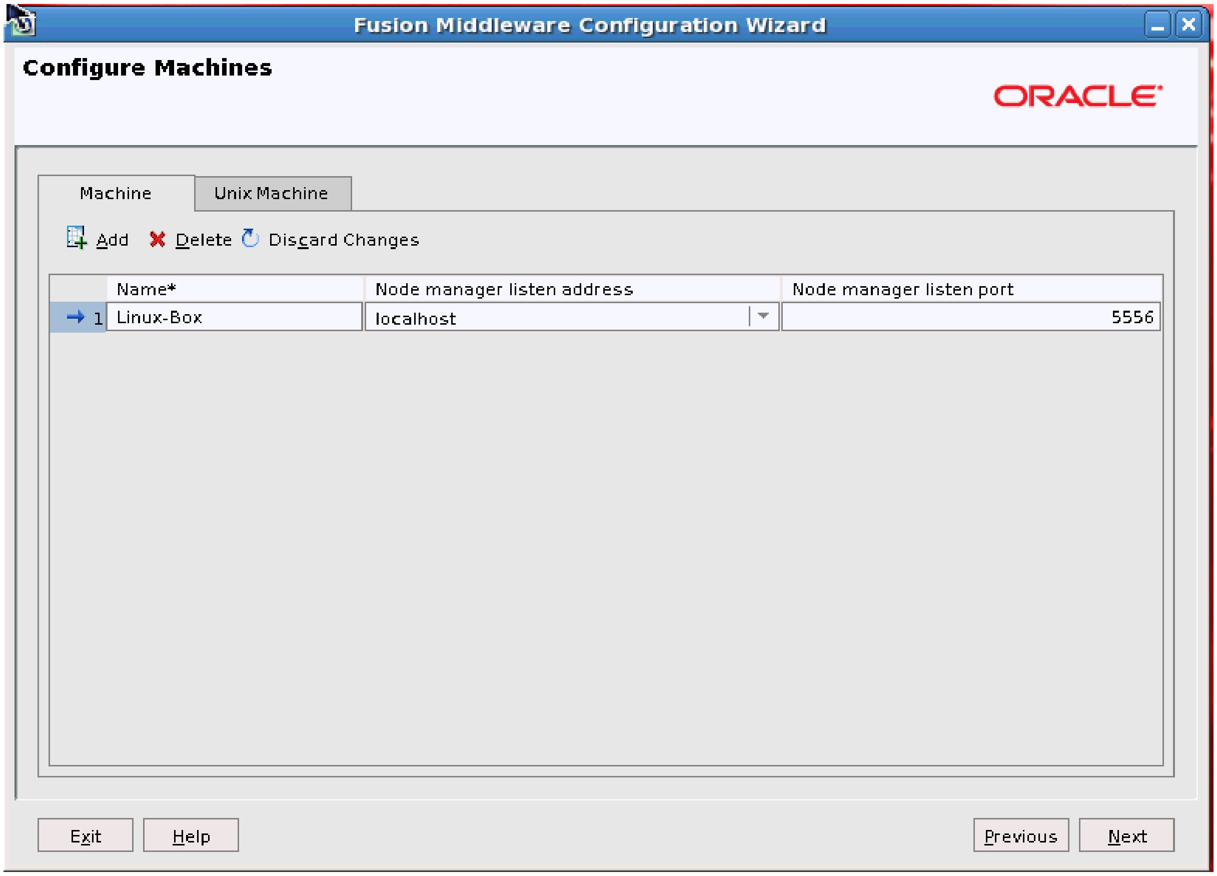
Select a cluster in the right pane. Then select the managed server(s) in the left pane and assign them to the cluster by clicking the right arrow button.

- cap_cluster
  - capture_server1
  - capture_server2

Assign two or more of the Managed Servers in the domain to each cluster.

Click **Next** to continue.

B.9 Configure Machines



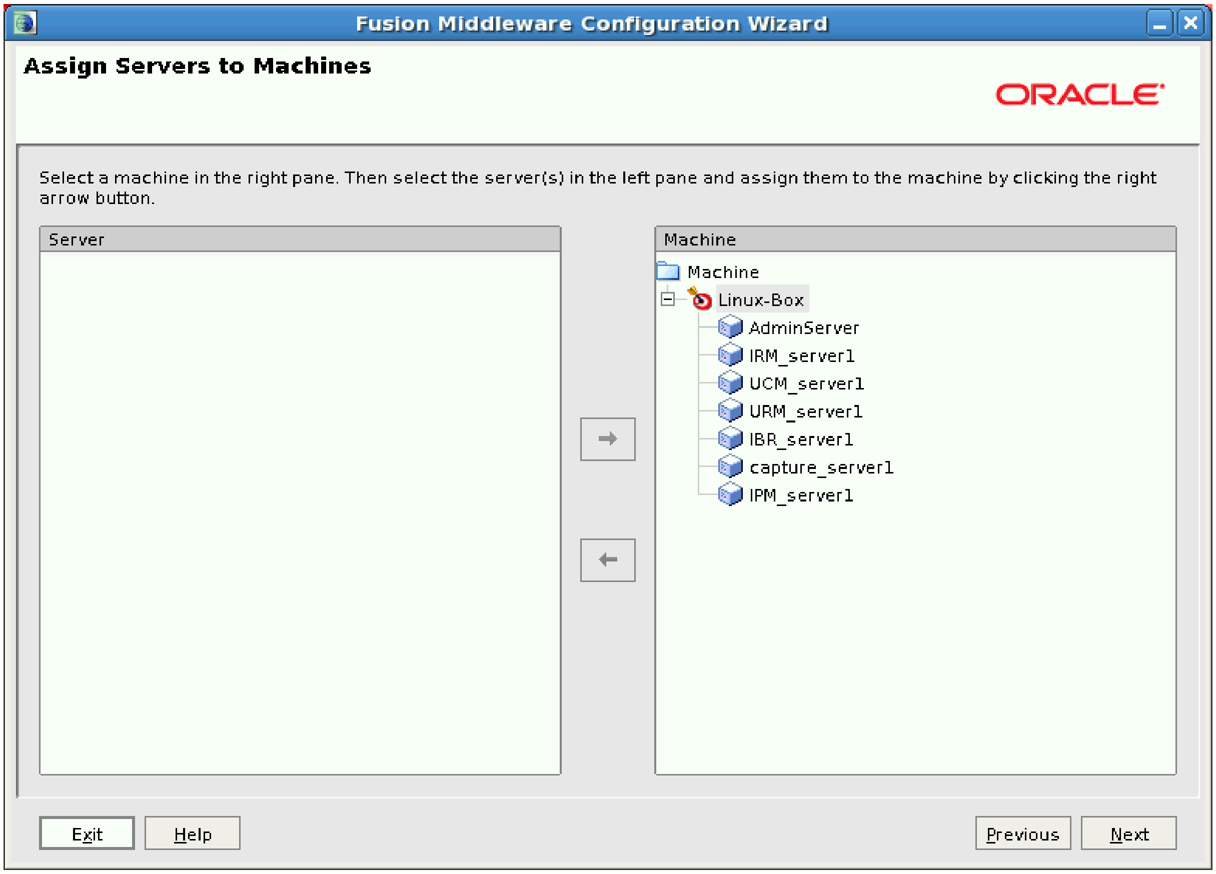
	Name*	Node manager listen address	Node manager listen port
1	Linux-Box	localhost	5556

Optionally, configure machines to host Managed Servers.

Click **Next** to continue.

Click **Next** to continue.

B.10 Assign Servers to Machines



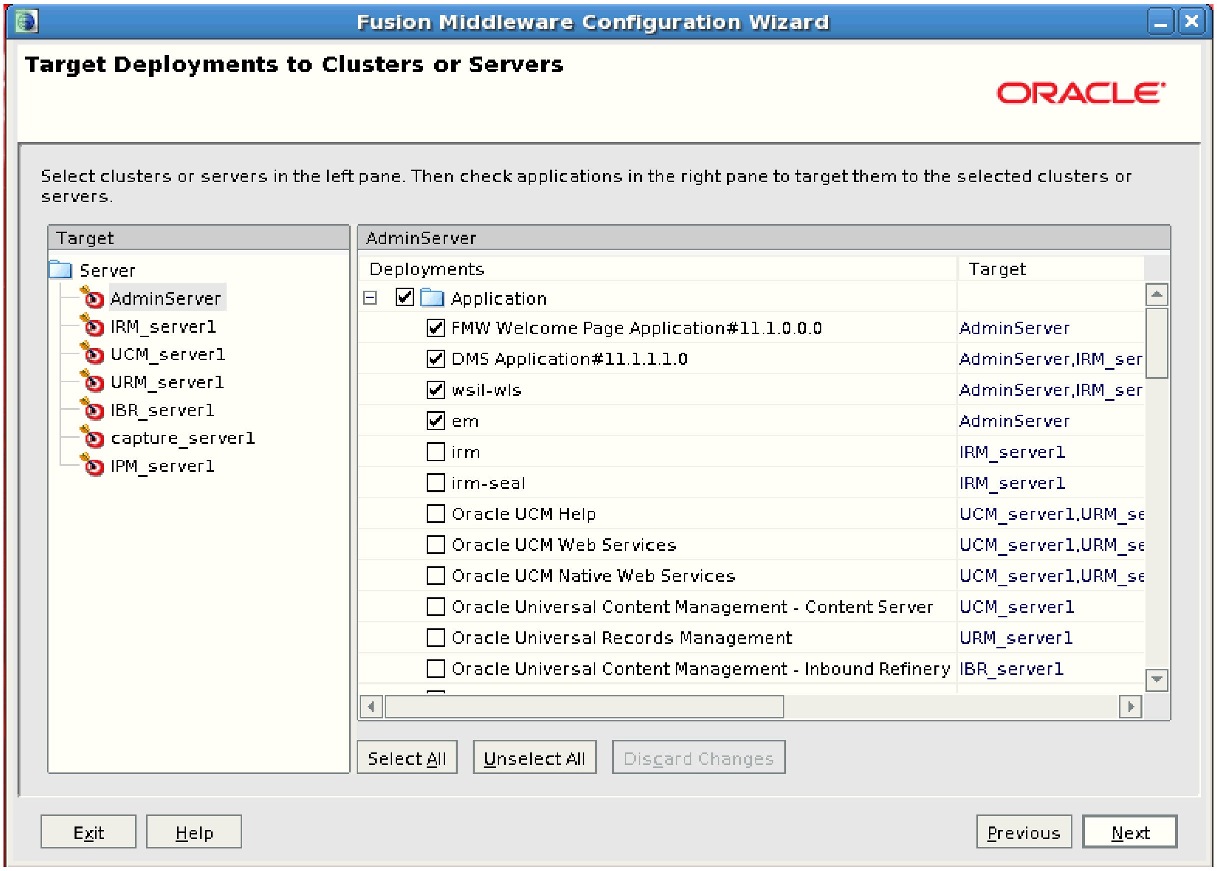
Assign Servers to Machines

Select a machine in the right pane. Then select the server(s) in the left pane and assign them to the machine by clicking the right arrow button.

Assign at least one server to each machine.

Click **Next** to continue.

B.11 Target Deployments to Clusters or Servers



Target Deployments to Clusters or Servers

Select clusters or servers in the left pane. Then check applications in the right pane to target them to the selected clusters or servers.

Target

- Server
  - AdminServer
  - IRM_server1
  - UCM_server1
  - URM_server1
  - IBR_server1
  - capture_server1
  - IPM_server1

AdminServer

Deployments	Target
⊟ ☑ Application	
☑ FMW Welcome Page Application#11.1.0.0.0	AdminServer
☑ DMS Application#11.1.1.1.0	AdminServer,IRM_ser
☑ wsil-wls	AdminServer,IRM_ser
☑ em	AdminServer
□ irm	IRM_server1
□ irm-seal	IRM_server1
□ Oracle UCM Help	UCM_server1,URM_se
□ Oracle UCM Web Services	UCM_server1,URM_se
□ Oracle UCM Native Web Services	UCM_server1,URM_se
□ Oracle Universal Content Management - Content Server	UCM_server1
□ Oracle Universal Records Management	URM_server1
□ Oracle Universal Content Management - Inbound Refinery	IBR_server1

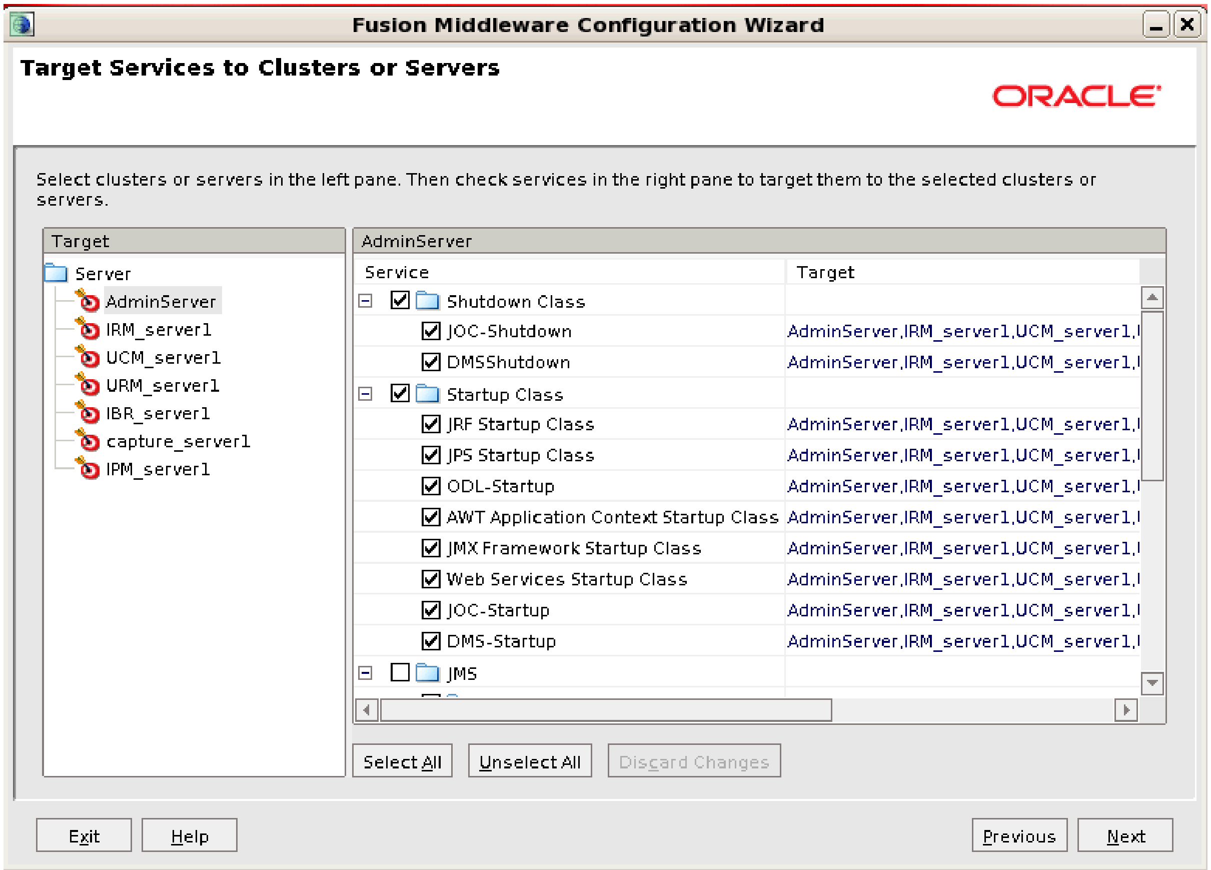
Optionally, assign each application to the Administration Server, a Managed Server, or a cluster of Managed Servers.

Oracle IRM should be deployed on a cluster or on a Managed Server that is not a member of any cluster because Oracle IRM uses `persistent-store-type` as `replicated_if_clustered`. If the Oracle IRM web application is deployed on a clustered server, the in-effect `persistent-store-type` value will be replicated. Otherwise, `memory` is the default.

When deploying Oracle IRM to a cluster, make sure that the Oracle IRM application is deployed to all nodes.

Click **Next** to continue.

B.12 Target Services to Clusters or Servers



Target Services to Clusters or Servers

Select clusters or servers in the left pane. Then check services in the right pane to target them to the selected clusters or servers.

Target

- Server
  - AdminServer
  - IRM_server1
  - UCM_server1
  - URM_server1
  - IBR_server1
  - capture_server1
  - IPM_server1

AdminServer

Service	Target
⊟ ☑ Shutdown Class	
☑ JOC-Shutdown	AdminServer,IRM_server1,UCM_server1,I
☑ DMSShutdown	AdminServer,IRM_server1,UCM_server1,I
⊟ ☑ Startup Class	
☑ JRF Startup Class	AdminServer,IRM_server1,UCM_server1,I
☑ JPS Startup Class	AdminServer,IRM_server1,UCM_server1,I
☑ ODL-Startup	AdminServer,IRM_server1,UCM_server1,I
☑ AWT Application Context Startup Class	AdminServer,IRM_server1,UCM_server1,I
☑ JMX Framework Startup Class	AdminServer,IRM_server1,UCM_server1,I
☑ Web Services Startup Class	AdminServer,IRM_server1,UCM_server1,I
☑ JOC-Startup	AdminServer,IRM_server1,UCM_server1,I
☑ DMS-Startup	AdminServer,IRM_server1,UCM_server1,I
⊟ ☐ JMS	

Optionally, modify how your services are targeted to servers or clusters.

Click **Next** to continue.

C

Deinstallation Screens for Oracle WebCenter Content

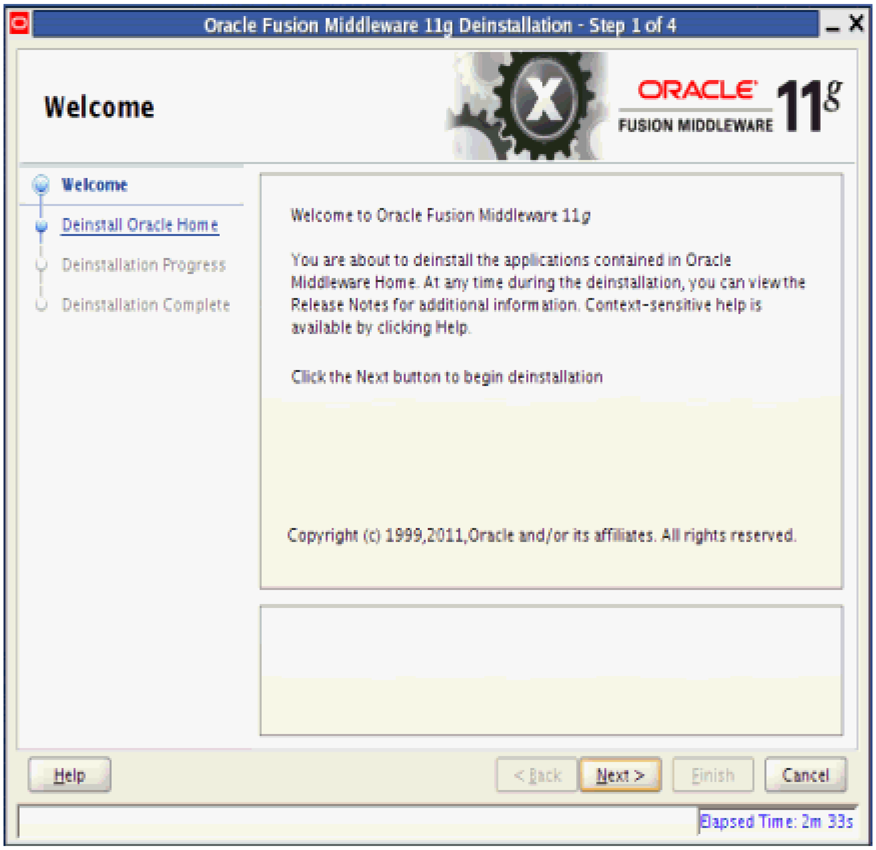
This appendix describes the Oracle Fusion Middleware 11*g* WebCenter Content Installer screens for uninstalling Oracle WebCenter Content from Oracle Fusion Middleware.

For information about how to remove an Oracle WebCenter Content installation, see Chapter 11, "Uninstalling Oracle WebCenter Content."

This appendix includes the following screens:

- Welcome
- Deinstall Oracle Home
- Deinstallation Progress
- Deinstallation Complete

C.1 Welcome



Welcome to Oracle Fusion Middleware 11*g*

You are about to deinstall the applications contained in Oracle Middleware Home. At any time during the deinstallation, you can view the Release Notes for additional information. Context-sensitive help is available by clicking Help.

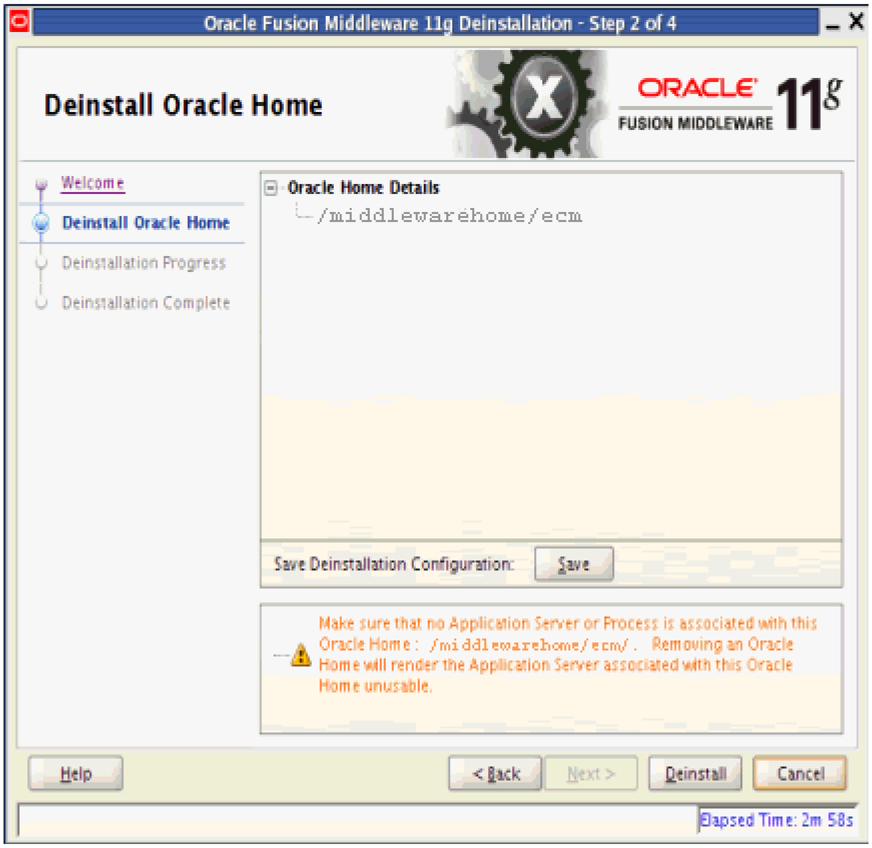
Click the Next button to begin deinstallation

Copyright (c) 1999,2011,Oracle and/or its affiliates. All rights reserved.

The Welcome screen is displayed each time you start the deinstaller.

Click **Next** to continue.

C.2 Deinstall Oracle Home



Oracle Home Details
/middlewarehome/ecm

Save Deinstallation Configuration: Save

Make sure that no Application Server or Process is associated with this Oracle Home : /middlewarehome/ecm/ . Removing an Oracle Home will render the Application Server associated with this Oracle Home unusable.

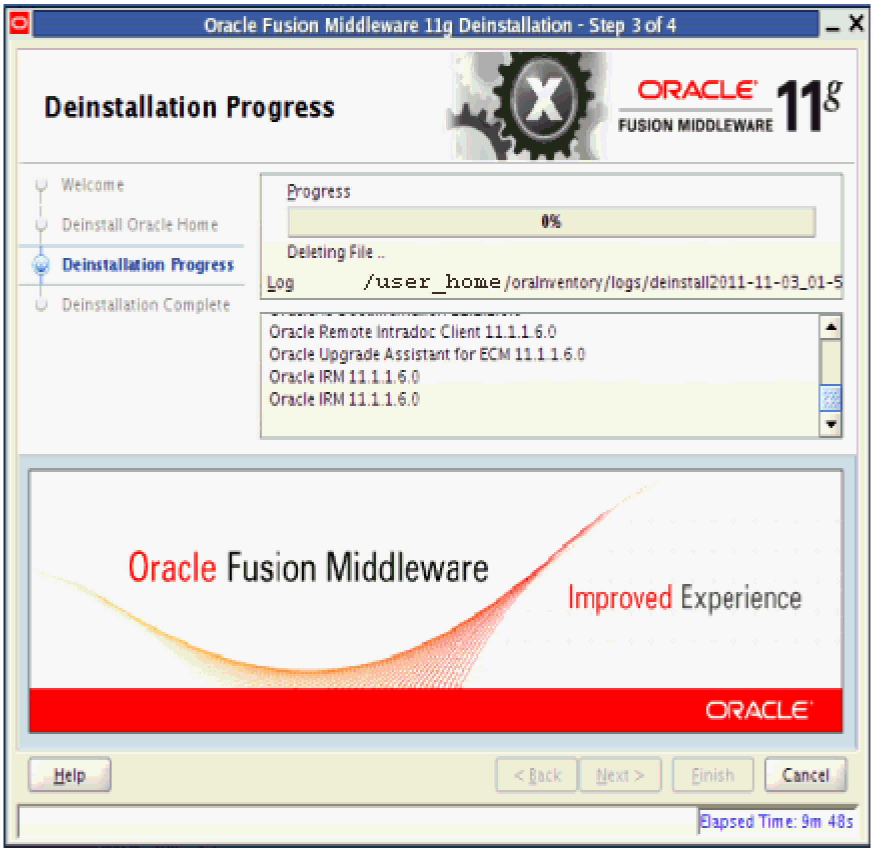
Elapsed Time: 2m 58s

This screen shows the Oracle home directory that is about to be uninstalled. 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



Progress

0%

Deleting File ..

Log /user_home/oraInventory/logs/deinstall2011-11-03_01-5

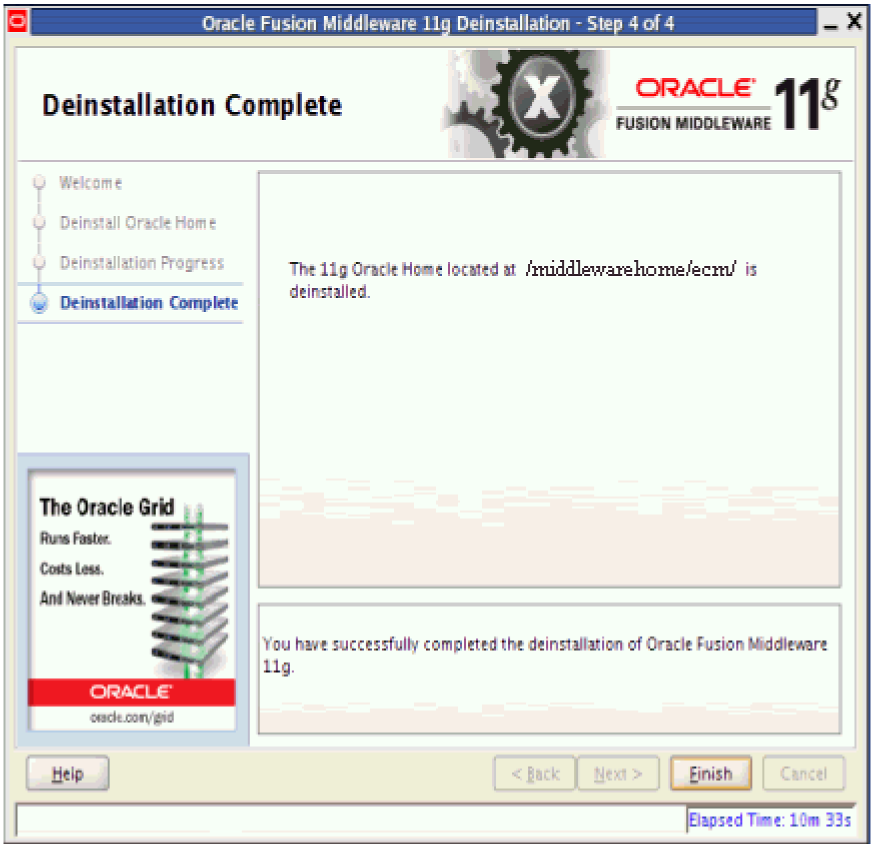
```
Oracle Remote Intradoc Client 11.1.1.6.0
Oracle Upgrade Assistant for ECM 11.1.1.6.0
Oracle IRM 11.1.1.6.0
Oracle IRM 11.1.1.6.0
```

Elapsed Time: 9m 48s

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



The 11g Oracle Home located at /middlewarehome/ecm/ is deinstalled.

You have successfully completed the deinstallation of Oracle Fusion Middleware 11g.

This screen summarizes the deinstallation that was just completed.

Click **Finish** to dismiss the screen.

D

Silent Installation

This appendix describes silent installation of Oracle WebCenter Content, without the graphical user interface.

You can install Oracle WebCenter Content from the command line, in silent mode, if you provide a response file with information specific to your installation. When you install Oracle WebCenter Content with the Oracle Fusion Middleware 11*g* WebCenter Content Installer, as described in Section 2.4, "Using the Installer for Oracle WebCenter Content," you can save a response file to perform a silent installation later.

For information about silent installation and deinstallation, see "Silent Installation and Deinstallation" in the *Installation Planning Guide*.

E

Oracle WebCenter Content: Desktop Configuration

This appendix describes the configuration tasks required to enable the use of Oracle WebCenter Content: Desktop.

This appendix includes the following sections:

- Section E.1, "Extracting and Running the Installation File for Your Desktop Client Software"
- Section E.2, "Setting the Web Browser Search Provider Name"
- Section E.3, "Enabling Subfolder Searching"
- Section E.4, "Mapping Email Metadata"
- Section E.5, "Configuring Form-Based Login"
- Section E.6, "Customizing the Form-Based Login Regular Expression"
- Section E.7, "Configuring Default Comments for New Check-Ins"

E.1 Extracting and Running the Installation File for Your Desktop Client Software

After Oracle WebCenter Content is installed, you can use the `desktop_content_setup.exe` command with the `/export` parameter to extract the Desktop installer files:

```
desktop_content_setup.exe /export [path/existing_extraction_directory/]
```

You can specify an existing directory to extract the files into. If you omit the directory from the command, it extracts the files into the current directory.

> **Note:** If you have an earlier version of Desktop installed, uninstall it before you proceed with the installation of Desktop 11.1.1.9.

The `desktop_content_setup.exe` command extracts three files:

- `package.ini`
- `contentdesktop.msi`
- `contentdesktop_x64.msi`

To install Desktop on a client system, use only one of the MSI files in the Desktop installer command.

The Desktop client software installers support a number of custom installation options that can help system administrators roll out the software:

- Section E.1.1, "Using Command-Line Parameters for Automation"
- Section E.1.2, "Disabling Integrations"
- Section E.1.3, "Performing Silent Roll-Outs"
- Section E.1.4, "Configuring Content Server Connections Through the Registry on a Windows System"

E.1.1 Using Command-Line Parameters for Automation

You can use several command-line parameters to automate part of the installation process. If you need to pass any public property to MSI through `desktop_content_setup.exe`, you can do that with the following command:

```
desktop_content_setup.exe /msi ONE_PUBLIC_PROPERTY=public_property_value
```

E.1.2 Disabling Integrations

The Desktop installer provides a number of command-line options to disable specific software integrations. If the installer detects that an integration can be applied to existing software on the computer (Microsoft Word, PowerPoint, Excel, and so on), it usually will automatically attempt to install an integration. To prevent an integration from being installed for a specific software product, you can disable that integration using one of these command-line switches:

- EXPLORER=0
- WORD=0
- POWERPOINT=0
- EXCEL=0
- OUTLOOK=0
- NOTES=0

Use capital letters for the switch names.

These switches are only for disabling software integrations. They are not necessary to enable software integrations for applications found on client computers.

E.1.3 Performing Silent Roll-Outs

The Desktop installer enables an administrator to roll out the Desktop client software to multiple client machines with the help of third-party tools such as SMS or netOctopus, which are capable of executing one executable on many machines. The installer for the Desktop client software supports a silent installation option that you can configure with SMS.

For silent install, you can use the following command to control the level of user interface displayed.

```
desktop_content_setup.exe /s UI=user_interface_level
```

In the command, *user_interface_level* can be 1, 2, 3, or 4:.

- 1: No user interface during install.
- 2: Displays only a progress bar during install.
- 3: Presents an install screen with different dialog boxes but does not require user input to run.
- 4: Runs a fully interactive installer requiring user input.

For example, to silently and selectively disable installing Outlook, PowerPoint, and Lotus Notes, the command would be as follows:

```
desktop_content_setup.exe /s UI=1 /msi OUTLOOK=0 POWERPOINT=0 NOTES=0
```

You will also need to add the REBOOT=ReallySuppress and MSIRESTARTMANAGERCONTROL=Disable properties to prevent reboots and to prevent any dialogs asking to shut down applications. For example:

```
desktop_content_setup.exe /s UI=2 /msi OUTLOOK=0
POWERPOINT=0 NOTES=0 REBOOT=ReallySuppress MSIRESTARTMANAGERCONTROL=Disable
```

The properties after the /msi switch can also be used with the *msiexec* with the MSI files. For example:

```
start /wait msiexec /i contentdesktop_x64.msi OUTLOOK=0 WORD=0 EXCEL=0
POWERPOINT=0 NOTES=0 REBOOT=ReallySuppress MSIRESTARTMANAGERCONTROL=Disable /l*v
DISUpgrade_x64.log /qn
```

E.1.4 Configuring Content Server Connections Through the Registry on a Windows System

You can add Content Server connections by creating a registry file on a Windows system. The file is not included as part of the standard installation files; you must create it.

Adding servers in a registry file automates the setup process by saving your users from setting up connections on their computers. When you add a server connection in this manner, the user cannot delete the server connection from their desktop (Windows Explorer, the email client, or any desktop application).

Sample Registry File Entries

The following sample registry file entries are examples for Content Servers instances, WebDAV servers, and Content DB servers, with comments below the code lines.

The sample file registry entries are under HKEY_LOCAL_MACHINE. If you would like the user to run the installer, use HKEY_CURRENT_USER instead of HKEY_LOCAL_MACHINE.

Using HKEY_LOCAL_MACHINE means that users cannot change the ServerAuth or RememberMetaData values because they will not have permission to change HKEY_LOCAL_MACHINE entries (unless a Windows policy is set to allow this, or the user is an administrator).

HKEY_LOCAL_MACHINE values override HKEY_CURRENT_USER values.

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\WebCenter
Desktop\Content\WebDAV\Servers\Corporate]
"ServerType"="ucm"
"ServerURL"="http://corporate/cs/idcplg/webdav"
```

(In this registry entry, the server is a Content Server instance, the display name of the server is `Corporate`, and the server WebDAV URL is `http://corporate/cs/idcplg/webdav`.)

```
[HKEY_LOCAL_MACHINE\Software\ORACLE\WebCenter
Desktop\Content\Shared\Config\Corporate]
"HostCgiUrl"="http://corporate/cs/idcplg"
"ServerAuth"=REG_DWORD:0x00000000 (0)
"RememberMetaData"=REG_DWORD:0x00000000 (0)
```

(In this registry entry, the server is a Content Server instance, the name of the server is `Corporate`, the CGI URL is `http://corporate/cs/idcplg`, and the user interface URL is `http://corporate/wcc/faces`. Content DB servers and WebDAV servers do not use these registry entries.)

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\WebCenter
Desktop\Content\WebDAV\Servers\Department]
"ServerType"="dav"
"ServerURL"="http://corporate/content/app/explorerPage.jspx"
"Single Sign-On Url"="http://section/content/app/explorerPage.jspx"
"Use Single Sign-On"=REG_DWORD:0x00000001 (1)
```

(In this registry entry, the server is a WebDAV server, the display name of the server is `Department`, the server WebDAV URL is `http://corporate/content/app/explorerPage.jspx`, a single sign-on page has been identified, and single sign-on has been implemented.)

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\WebCenter
Desktop\Content\WebDAV\Servers\Section]
"ServerType"="cdb"
"ServerURL"="http://section/content/dav"
"Single Sign-On Url"="http://section/content/app/explorerPage.jspx"
"Use Single Sign-On"=REG_DWORD:0x00000001 (1)
```

(In this registry entry, the server is a Content DB server, the display name of the server is `Section`, the server WebDAV URL is `http://section/content/dav`, a single sign-on page has been identified, and single sign-on has been implemented.)

E.2 Setting the Web Browser Search Provider Name

Desktop provides plug-ins for various popular web browsers which enable users to search for content on a Content Server instance directly from the search field in their web browser.

The default search provider name for an Oracle WebCenter Content Server instance is *Oracle WebCenter Content Search*, but this can be modified to a more meaningful name for the server.

To modify the default search provider name:

1. Log in to Content Server as an administrator.
2. Choose **Administration** then **Configuration for *SERVER***.
3. On the Configuration page, in **Features And Components**, click **Enabled Component Details**.
4. In the list of installed components, find **DesktopIntegrationSuite** and click its **Configure** link.

5. On the Update Component Information page, make sure the **Enable web browser search plug-in** checkbox is selected.
6. Enter the search provider name for the server in the **Web browser search plug-in title** field. Choose a search provider name that is unique across the organization. Two servers with the same search provider name are not allowed.
7. When done, click **Update** to enable the new settings, **Reset** to cancel any modifications, or **Revert To Install Settings** to return to all default settings.
8. Restart Content Server.

E.3 Enabling Subfolder Searching

If a Content Server instance is using Framework Folders as the content hierarchy component, subfolder searching can be enabled. This allows users to specify whether a content search should apply to the current folder only or whether it should include all subfolders of that folder.

To enable subfolder searching, Content Server must be configured to use the Oracle Text Search engine, and some elements must be added to the search form.

To enable subfolder searching:

1. Log in to the WebLogic Server Administration Console for Content Server.
2. Choose **General Configuration**.
3. On the General Configuration page, verify that the **Additional Configuration Values** section includes the following entries:

```
SearchIndexerEngineName=OracleTextSearch
FoldersIndexParentFolderValues=true
```

4. Click **Save**.
5. Restart Content Server.
6. Rebuild the search collection index.

The content search form now includes a Parent Folder field as well as an **Include Subfolders** checkbox, which allows users to limit a search query to just the current content folder or expand it to include all subfolders.

E.4 Mapping Email Metadata

Administrators can map email header fields to metadata fields for messages checked in to Content Server. MSG metadata mapping is used for the Microsoft Outlook message format and EML metadata mapping for Internet mail message format.

The six standard email metadata mappings cannot be overridden. Only additional mappings can be created.

To map email metadata:

1. Log in to Content Server as an administrator.
2. Choose **Administration** then **Configure Email Metadata** then **Map MSG Metadata** or **Map EML Metadata**.

3. On the Email Metadata Mappings page, the listed email header fields under **Available Fields** are not mapped and the fields under **Mapped Fields** are mapped to metadata. Use the right and left arrows to select a field and move it from one group to the other. Use the up and down arrows to sort the fields within each grouping.
4. As fields are added to or removed from **Mapped Fields**, a drop-down list appears for that field under **Mapped Values**. For each mapped email header field, select a value for the metadata field from the dropdown list.
5. When all fields are updated with metadata values, click **Save**.

E.5 Configuring Form-Based Login

Your organization may use separate identity and access management software that provides secure, form-based login screens to authenticate users and control access. Desktop is compatible with form-based logins. To enable this, add a comment to the login page so Desktop identifies an HTML response as the forms-based login page. Users will see the form-based login instead of the standard content server login.

To configure form-based login:

1. Locate the login form on the file system (for example, `login.fcc` for Netegrity SiteMinder). The location of this form depends on how the authentication system was set up.
2. Open the form in a text editor.
3. Add the following comment (with no spaces) to the HEAD section of the form:

   ```
   <!--IdcClientLoginForm=1-->
   ```

   > **Important:** The form's HEAD section may contain a great deal of code. The delivered page must have that HTML comment (or token) in the first 5,000 characters of the response. If not, the server connection may fail.
   >
   > The software on the client computer checks the response for the `<!--IdcClientLoginForm=1-->` token (using a strict string search) and route through the prompting code if it is found. It is encoded as an HTML comment so that regular browsers do not show the token when they attempt to log in. If it is Idoc Script, then the parser removes that bit of code from the delivered page, and the client-side browser will not see anything in the page.

4. Save and close the form.

E.6 Customizing the Form-Based Login Regular Expression

By default, Desktop uses the following regular expression to identify a form-based login:

```
<!--IdcClientLoginForm=1-->|
<form .*sso.* name=\"LoginForm\"|
<form *name=\"loginForm\"
```

This regular expression is configurable in the Windows Registry. The code first looks in the following place:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\WebCenter
Desktop\Content\WebDAV\Servers\SERVER_NAME]
"Form Based Logins Reg Exp"="REGULAR_EXPRESSION"
```

Then it looks here:

```
[HKEY_CURRENT_USER\SOFTWARE\Oracle\WebCenter
Desktop\Content\WebDAV\Servers\SERVER_NAME]
"Form Based Logins Reg Exp"="REGULAR_EXPRESSION"
```

Then it looks here:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\WebCenter Desktop\Content\WebDAV]
"Form Based Logins Reg Exp"="REGULAR_EXPRESSION"
```

Finally it looks here:

```
[HKEY_CURRENT_USER\SOFTWARE\Oracle\WebCenter Desktop\Cotnent\WebDAV]
"Form Based Logins Reg Exp"="REGULAR_EXPRESSION"
```

If no custom regular expression is defined in any of these Windows Registry locations, the default one is used.

E.7 Configuring Default Comments for New Check-Ins

By default, the Desktop client does not have a default comment for new check-ins. You can configure the DesktopIntegrationSuite component to have a default comment.

The configuration fields for the default check-in comment follow:

- **Check-in dialog comment metadata field name**

  This is the name of the metadata field returned by the service call to use as the default comment. The default value for this field is `xComments`.

- **Check-in dialog default comment**

  This string will be used as the default comment if one is not obtained from a service call.

- **Check-in dialog comment service**

  This is the service call used to obtain the comment.

- **Maximum check-in dialog comment length**

  This is the maximum length of the comment. If this value is not specified, the length of the field returned by the service call will be used.

For the simplest configuration, set **Check-in dialog comment service** to `DOC_INFO`, and leave the **Check-in dialog comment metadata field name** as `xComments`. This will obtain the previous comment from the server when the item is checked out.

You can configure the component so that it will make a custom service call into a custom component to obtain the default comment. The comment could be based on the file name or the user name or some other metadata associated with the content item.

F

Troubleshooting

This appendix provides troubleshooting information.

This appendix includes the following sections:

- Section F.1, "General Troubleshooting Tips"
- Section F.2, "Oracle WebCenter Content Installation and Configuration Troubleshooting"
- Section F.3, "Inbound Refinery Problems"
- Section F.4, "Additional Help"

F.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/technetwork/documentation`

- Verify that your system meets the requirements specified in Section 2.1.3, "Reviewing System Requirements and Certification".
- If you are installing a middle tier, check that the OracleAS Infrastructure with which you want to associate the middle tier is running during installation.
- If you entered incorrect information on one of the installation screens, return to that screen by clicking **Back** until you see the screen.
- If an error occurred while the installer is copying or linking files:

  1. Note the error and review the installation log files.
  2. Remove the failed installation by following the steps in Chapter 11, "Uninstalling Oracle WebCenter Content."
  3. Correct the issue that caused the error.
  4. Restart the installation.

F.2 Oracle WebCenter Content Installation and Configuration Troubleshooting

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

If you are having problems with full-text search, Inbound Refinery conversions, Dynamic Converter, Oracle WebCenter Content: Desktop, or Content Categorizer on a Windows operating system, first make sure you have downloaded the correct version of the Visual C++ Redistributable Package, as described in Section 3.7.3, "Downloading Visual C++ Libraries for a Windows Operating System."

This section provides troubleshooting information for the following Oracle WebCenter Content installation and configuration issues:

- Oracle Fusion Middleware Installation and Configuration Log Files
- Oracle IRM Keystore Configuration Issues
- Imaging Errors During Attempt to Connect to WebCenter Content 11g
- Imaging Errors from AXF If Oracle SOA Suite Not Installed
- Content Server Errors Connecting to Oracle WSM Policy Manager in Domain with Oracle SOA Suite or Oracle BAM

F.2.1 Oracle Fusion Middleware Installation and Configuration Log Files

The Oracle Fusion Middleware 11*g* WebCenter Content Installer and Fusion Middleware Configuration Wizard create their own sets of log files.

- On a UNIX operating system, the installer writes the following log files:
  - `oraInventory_location/logs/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.

F.2.2 Oracle IRM Keystore Configuration Issues

If the Oracle Information Rights Management keystore 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 keystore file

  If the keystore 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 keystore 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
  ```

F.2.3 Imaging Errors During Attempt to Connect to WebCenter Content 11g

When you attempt to connect Oracle WebCenter Content: Imaging to a WebCenter Content 11*g* repository, Imaging returns errors in these cases:

- If WebCenter Content is installed in a domain that is later extended with Imaging and you have not restarted the Imaging Managed Server.
- If the WebCenter Content and Imaging Managed Servers are configured to run on different machines and you have not performed the manual configuration.

For information about avoiding these errors, see Section 6.1.1.1, "Configuring WebCenter Content 11g to Work with Imaging."

F.2.4 Imaging Errors from AXF If Oracle SOA Suite Not Installed

If you use Oracle WebCenter Content: Imaging without Oracle SOA Suite in a single-machine environment, Imaging generates errors AXF errors when you start the Imaging Managed Server. The AXF product require Oracle SOA Suite to be installed in the same WebLogic Server domain as Oracle WebCenter Content in a single-machine environment. You can ignore these errors if you do not plan to use AXF for BPEL or AXF for BPM with Imaging.

You can also get these AXF errors if the Oracle SOA Suite Managed Server is not running when you start the Imaging Managed Server.

For more information, see Chapter 6, "Completing the Imaging Configuration."

F.2.5 Content Server Errors Connecting to Oracle WSM Policy Manager in Domain with Oracle SOA Suite or Oracle BAM

If you get connection errors from Web Services Manager (Oracle WSM) Policy Manager when you start Oracle WebCenter Content Server in a domain that includes Oracle SOA Suite or Oracle Business Activity Monitoring (Oracle BAM), you need to start the Oracle SOA Suite or Oracle BAM Managed Server before you start the WebCenter Content Managed Server.

Oracle WSM is configured during domain creation or extension for Content Server to connect to the Policy Manager. You need to start either Oracle SOA Suite or Oracle BAM first so Content server can make these connections.

For more information, see Section 3.14, "Setting Up Oracle Web Services Manager Security."

F.2.6 Missing Files Error When Starting Records Server Connected to Microsoft SQL Server

If you are using a Microsoft SQL Server database with Oracle WebCenter Content: Records, you can safely ignore any errors with the following text that occur when the Records Managed Server is started:

```
Failed to find indexable webviewable for content item panel
```

This text refers to panels used by the Records dashboard for the user. By design, these panels do not have web-viewable interfaces that are indexable. Their content is derived when they are run at display time.

F.3 Inbound Refinery Problems

If you are having problems with Inbound Refinery conversions on a Windows operating system, first make sure you have downloaded the correct version of the Visual C++ Redistributable Package, as described in Section 3.7.3, "Downloading Visual C++ Libraries for a Windows Operating System."

This section provides troubleshooting information for the following Inbound Refinery setup and run issues:

- Cannot Log In to Refinery After Installation
- Files Intermittently Stuck in GenWWW Status
- RIDC Port Not Set on First Inbound Refinery Startup

F.3.1 Cannot Log In to Refinery After Installation

When you attempt to log in to a refinery after installation, you get an error similar to the following one:

```
"Content Server Access Denied
Access denied to Content Server managed resource. Error getting user credentials
from proxied user cache. Unable to open file
c:/ucm/cs1/data/users/proxied/ref1/userdb.txt.
 c:/ucm/cs1/data/users/proxied/ref1/userdb.txt contains an invalid path."
```

Possible Causes	Solutions
The refinery has been proxied to Content Server, but the `InboundRefinerySupport` component has not been installed and enabled on Content Server.	Install and enable the `InboundRefinerySupport` component on Content Server. For more information, see Section 5.2.3.2, "Enabling Components for Inbound Refinery on Content Server."

F.3.2 Files Intermittently Stuck in GenWWW Status

When WebCenter Content is run on a Windows Server 2003 system, files intermittently get stuck in GenWWW. There are no conversion errors, and when resubmitted, the files are successfully converted.

Possible Causes	Solutions
The problem is directly related to known file locking and deleting issues on a Windows Server 2003 system and typically occurs when Content Server runs on a UNIX operating system and Samba is used to connect to the Windows Server 2003 machine. However, the problem can also occur when you are using Inbound Refinery on the Windows Server 2003 system and Inbound Refinery resides on a separate physical machine from Content Server. For more information about these Windows Server 2003 issues, see knowledge base articles 885451 and 811492 on the Microsoft Support website at `http://support.microsoft.com`	To confirm that you are experiencing the issues described in Microsoft's knowledge base articles, delete several files on your Windows Server 2003 machine using a remote client. If you witness a delay of up to 40 seconds in the file deletion, it is likely that the Windows Server 2003 locking/deleting issue is the problem. Microsoft offers two solutions to this issue. **1.** Microsoft has a hotfix for Windows Server 2003 that can be shipped on a request-only basis. However, Microsoft's recommendation is to wait until the next service pack unless you are 'severely' affected by the problem. **2.** The alternate solution from Microsoft is to disable *opportunistic locking* on the Windows Server 2003 server. The solution to disable opportunistic locking does not impact the normal file locking used when writing a file. Rather, opportunistic locking is a speed tweak to the file locking process that can be safely disabled if it is causing problems. Additional information on opportunistic locks is contained in the Samba help files. If you need specific information on how to disable opportunistic locking on a Windows Server 2003 server, see knowledge base article 29624 on the Microsoft Support website at `http://support.microsoft.com`

F.3.3 RIDC Port Not Set on First Inbound Refinery Startup

The first time you start the Oracle WebCenter Content: Inbound Refinery Managed Server, Inbound Refinery generates an `RIDC port not set` exception.

The Remote Intradoc Client (RIDC) port is configured after you complete the initial configuration of Inbound Refinery and restart the Inbound Refinery Managed Server. Inbound Refinery should not generate this exception after it is configured and restarted.

For more information, see Section 5.1, "Completing the Initial Inbound Refinery Configuration."

F.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/technetwork/documentation`

- My Oracle Support (formerly Oracle*MetaLink*) website at

  `http://support.oracle.com`

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

Index