Oracle® Fusion Middleware

Installing and Configuring Oracle WebCenter Content

14c (14.1.2.0.0)
F85510-01
December 2024

Oracle Fusion Middleware Installing and Configuring Oracle WebCenter Content, 14c (14.1.2.0.0)

F85510-01

Primary Author: Oracle Corporation

Contents

E Updating the JDK After Installing and Configuring an Oracle Fusion Middleware Product

Preface

This document describes how to install and configure Oracle WebCenter Content.

Audience

This guide is intended for system administrators or application developers who are installing and configuring Oracle WebCenter Content. It is assumed that readers are familiar with web technologies and have a general understanding of Windows and UNIX platforms.

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.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Related Documents

Refer to the Oracle Fusion Middleware Library for additional information.

- For Oracle WebCenter Content information, see Oracle WebCenter Content Documentation.
- For installation information, see Fusion Middleware Installation Documentation.
- For upgrade information, see Fusion Middleware Upgrade Documentation.
- For administration-related information, see Fusion Middleware Administration Documentation.
- For release-related information, see Fusion Middleware Release Notes.

Conventions

Learn about the conventions used in this document.

This document uses the following text conventions:

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

1

About the Oracle WebCenter Content Installation

The standard installation for Oracle WebCenter Content described in this guide creates the standard topology, which represents a sample starting topology for this product.

Using the Standard Installation Topology As a Starting Point

The standard installation topology is a flexible topology that you can use as a starting point in production environments.

If required, you can later extend the standard installation topology to create a secure and highly available production environment, see Next Steps After Configuring the Domain.

The standard installation topology represents a sample topology for this product. It is not the only topology that this product supports. See About the Standard Installation Topology in *Planning an Installation of Oracle Fusion Middleware*.

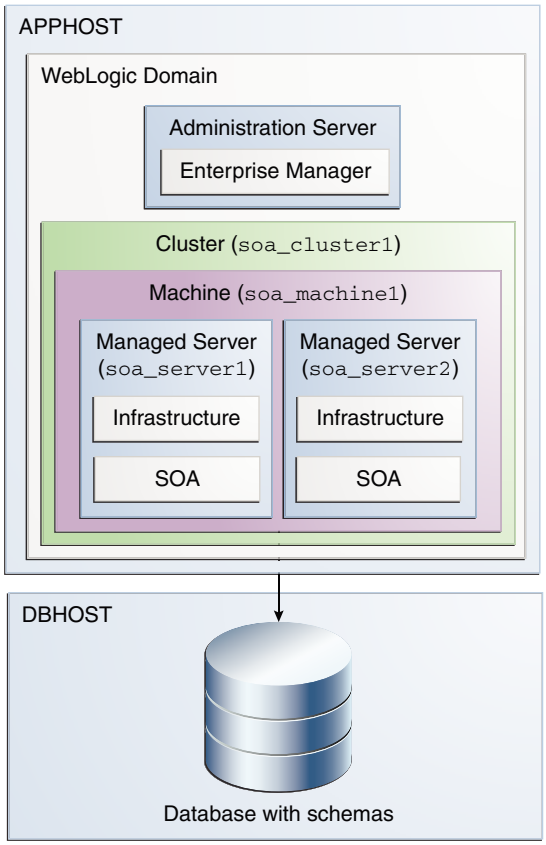
About the WebCenter Content Standard Installation Topology

This topology represents a standard WebLogic Server domain that contains an Administration Server and a cluster that contains two Managed Servers.

The following figure shows the standard installation topology for WebCenter Content.

See Table 1-1 for information on the elements for this topology.

Figure 1-1 Standard Installation Topology for Oracle WebCenter Content



About Elements in the Standard Installation Topology Illustration

The standard installation topology typically includes common elements.

Table 1-1 describes all elements of the topology illustration:

Table 1-1 Description of Elements in Standard Installation Topologies

Element	Description and Links to Related Documentation
APPHOST	A standard term used in Oracle documentation to refer to the machine that hosts the application tier.
DBHOST	A standard term used in Oracle documentation to refer to the machine that hosts the database.
WebLogic Domain	A logically related group of Java components (in this case, the Administration Server, Managed Servers, and other related software components) and non-Java components. See What Is an Oracle WebLogic Server Domain? in *Understanding Oracle Fusion Middleware*.
Administration Server	Central control entity of a WebLogic domain. It maintains configuration objects for that domain and distributes configuration changes to Managed Servers. See What Is the Administration Server? in *Understanding Oracle Fusion Middleware*.
Enterprise Manager	The Oracle Enterprise Manager Fusion Middleware Control is a primary tool used to manage a domain. See Oracle Enterprise Manager Fusion Middleware Control in *Understanding Oracle Fusion Middleware*.
Cluster	A collection of multiple WebLogic Server instances running simultaneously and working together. See Overview of Managed Servers and Managed Server Clusters in *Understanding Oracle Fusion Middleware*.

Table 1-1 (Cont.) Description of Elements in Standard Installation Topologies

Element	Description and Links to Related Documentation
Machine	A logical representation of the computer that hosts one or more WebLogic Server instances (servers). Machines are also the logical glue between the Managed Servers and the Node Manager. In order to start or stop the Managed Servers using the Node Manager, associate the Managed Servers with a machine.
Managed Server	A host for your applications, application components, web services, and their associated resources. See Overview of Managed Servers and Managed Server Clusters in *Understanding Oracle Fusion Middleware*.
Infrastructure	A collection of services that include the following: • Metadata repository (MDS) contains the metadata for Oracle Fusion Middleware components, such as the Oracle Application Developer Framework. See What Is the Metadata Repository? in *Understanding Oracle Fusion Middleware*. • Oracle Application Developer Framework (Oracle ADF). • Oracle Web Services Manager (OWSM).

About Installing Oracle User Messaging Service

Oracle User Messaging Service (UMS) is a software technology that enables two-way communication between users and deployed applications.

See Introduction to Oracle User Messaging Service in *Administering Oracle User Messaging Service*.

UMS is included in the Oracle Fusion Middleware Infrastructure distribution. It installs as part of the Oracle Fusion Middleware Infrastructure standard installation topology, as described in About Installing Oracle User Messaging Service (UMS) in *Installing and Configuring the Oracle Fusion Middleware Infrastructure* .

UMS runtime components consist of an Oracle Fusion Middleware Configuration Wizard template and an Oracle Fusion Middleware schema, which is installed into a supported database by using the Repository Creation Utility (RCU).

For development, you can install and use Oracle JDeveloper14*c* to develop applications that can take advantage of UMS features. See Introducing Oracle JDeveloper in *Installing Oracle JDeveloper*.

About Oracle WebCenter Content Scale Up

Oracle WebCenter Content supports only one Inbound Refinery Managed Server per node per domain, and one WebCenter Content Managed Server per node, per domain.

You cannot scale up Inbound Refinery or WebCenter Content. To add Managed Servers in a cluster, see Scaling Out a Topology (Machine Scale Out)in the *Oracle Fusion Middleware High Availability Guide* to add a Managed Server to a new node.

Using This Document to Extend an Existing Domain

The procedures in this guide describe how to create a new domain. The assumption is that no other Oracle Fusion Middleware products are installed on your system.

If you have installed and configured other Oracle Fusion Middleware products on your system (for example, Fusion Middleware Infrastructure, with a domain that is up and running) and wish

to extend the same domain to include Oracle WebCenter Content, see Installing Multiple Products in the Same Domain.

2

Preparing to Install and Configure Oracle WebCenter Content

To prepare for your Oracle WebCenter Content installation, verify that your system meets the basic requirements, then obtain the correct installation software.

Mandatory Steps for Installing WebCenter Content on Windows Operating Systems

There are three mandatory procedures that you must run before you install Oracle WebCenter Content.

Disabling the 8.3 File Naming Convention on a Windows Operating System

Before you install Oracle WebCenter Content on a Windows Operating System, you must 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 conflict with revision labels, causing 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 to make the change take effect.

Downloading Visual C++ Libraries

WebCenter Content and Inbound Refinery require the Visual C++ libraries included in Microsoft's Visual C++ Redistributable Package.

> **Note:**
>
> For a list of platforms that support PDF Searchable Document Output Format, go to the Oracle Fusion Middleware Supported System Configurations page. In the table, on the row **Oracle Fusion Middleware certifications**, select the **System Requirements and Supported Platforms for WebLogic Server** (14.1.2.0.0) (.xls) file.

Downloading Microsoft .Net Framework 4.x

The WinNativeConverter uses vb.Net code, so it requires Microsoft .NET Framework 4.x.

Download Microsoft .NET Framework 4.x at http://www.microsoft.com/downloads

Roadmap for Installing and Configuring the Standard Installation Topologies

Installing and configuration standard installation topology requires certain steps.

This document has all steps required to install and configure standard installation topologies. The guide also refers to additional information that you can use if you want to create a modified version of this topology.

The following table shows the steps required to install and configure the topology.

Table 2-1 Standard Installation Roadmap

Task	Description	Documentation
Verify your system environment	Before beginning the installation, verify that the minimum system and network requirements are met.	See Roadmap for Verifying Your System Environment.
Check for any mandatory patches that will be required before or after the installation	Review the Oracle Fusion Middleware Infrastructure release notes to see if there are any mandatory patches required for the software products you are installing.	See Install and Configure in *Release Notes for Oracle Fusion Middleware Infrastructure*.
Obtain the appropriate distributions	Install Oracle Fusion Middleware Infrastructure to create the Oracle Home for Oracle WebCenter Content	See About Product Distributions.
Determine your installation directories	Verify that the installer can access or create the installer directories that it must access or create. Also, verify that the directories exist on systems that meet the minimum requirements.	See What are the Key Oracle Fusion Middleware Directories? in *Understanding Oracle Fusion Middleware*.
Install prerequisite software	Install Oracle Fusion Middleware Infrastructure to create the Oracle home directory.	For Oracle Fusion Middleware Infrastructure , see*Installing and Configuring the Oracle Fusion Middleware Infrastructure*. You only need to perform the installation for Infrastructure. You do not need to configure a domain for Infrastructure.
Install the software	Run the Oracle Universal Installer to install Oracle WebCenter Content. Installing the software transfers the software to your system and creates the Oracle home directory.	See Installing the Oracle WebCenter Content Software.
Select a database profile and review any required custom variables.	Before you install required schemas in the database, review the information about any custom variables you will need to set for the Oracle WebCenter Content schemas.	See About Database Requirements for an Oracle Fusion Middleware Installation.

Table 2-1 (Cont.) Standard Installation Roadmap

Task	Description	Documentation
Create the schemas	Run the Repository Creation Utility to create the schemas required for configuration.	See Creating the Database Schemas.
Create a WebLogic domain	Use the Configuration Wizard to create and configure the WebLogic domain.	See Configuring the Domain if you are creating the topology for Oracle WebCenter Content.
Administer and prepare your domain for high availability	Discover additional tools and resources to administer your domain and configure your domain to be highly available.	See Next Steps After Configuring the Domain.

Roadmap for Verifying Your System Environment

Before you begin the installation and configuration process, you must verify your system environment.

Table 2-2 identifies important tasks and checks to perform to ensure that your environment is prepared to install and configure Oracle WebCenter Content.

Table 2-2 Roadmap for Verifying Your System Environment

Task	Description	Documentation
Verify certification and system requirements.	Verify that your operating system is certified and configured for installation and configuration.	See Verifying Certification, System, and Interoperability Requirements.
Identify a proper installation user.	Verify that the installation user has the required permissions to install and configure the software.	See Selecting an Installation User.
Select the installation and configuration directories on your system.	Verify that you can create the necessary directories to install and configure the software, according to the recommended directory structure. Select a new, empty Oracle Home directory.	See About the Directories for Installation and Configuration.
Install a certified JDK.	The installation program for the distribution requires a certified JDK present on your system.	See About JDK Requirements for an Oracle Fusion Middleware Installation.
Install and configure a database for mid-tier schemas.	To configure your WebLogic domain, you must have access to a certified database that is configured for the schemas required by Oracle WebCenter Content.	See About Database Requirements for an Oracle Fusion Middleware Installation.

Verifying Certification, System, and Interoperability Requirements

Oracle recommends that you use the certification matrix and system requirements documents with each other to verify that your environment meets the requirements for installation.

1. **Verifying that your environment meets certification requirements:**

Ensure that you install your product on a supported hardware and software configuration.

Oracle has tested and verified the performance of your product on all certified systems and environments. Whenever new certifications are released, they are added to the certification document right away. New certifications can be released at any time. Therefore, the certification documents are kept outside the documentation libraries and are available on Oracle Technology Network.

2. **Using the system requirements document to verify certification:**

   Oracle recommends that you use the *Oracle Fusion Middleware System Requirements and Specifications* document to verify that the certification requirements are met. System requirements can change in the future. Therefore, the system requirement documents are kept outside of the documentation libraries and are available on Oracle Technology Network.

3. **Verifying interoperability among multiple products:**

   To learn how to install and run multiple Fusion Middleware products from the same release or mixed releases with each other, see Oracle Fusion Middleware Interoperability and Compatibility in *Understanding Interoperability and Compatibility*.

Selecting an Installation User

The user who installs and configures your system must have the required permissions and privileges.

About User Permissions

The user who installs a Fusion Middleware product owns the files and has certain permissions on the files.

- Read and write permissions on all non-executable files (for example, `.jar`, `.properties`, or `.xml`). All other users in the same group as the file owner have read permissions only.
- Read, write, and execute permissions on all executable files (for example, `.exe`, `.sh`, or `.cmd`). All other users in the same group as the file owner have read and execute permissions only.

This means that someone other than the person who installs the software can use the installed binaries in the Oracle home directory to configure a domain or set of Fusion Middleware products.

During configuration, the files generated by the configuration process are owned by the user who ran the Configuration Wizard. This user has the same permissions as described above for the installation user. However, security-sensitive files are not created with group permissions. Only the user that created the domain has read and write permissions and can administer the domain.

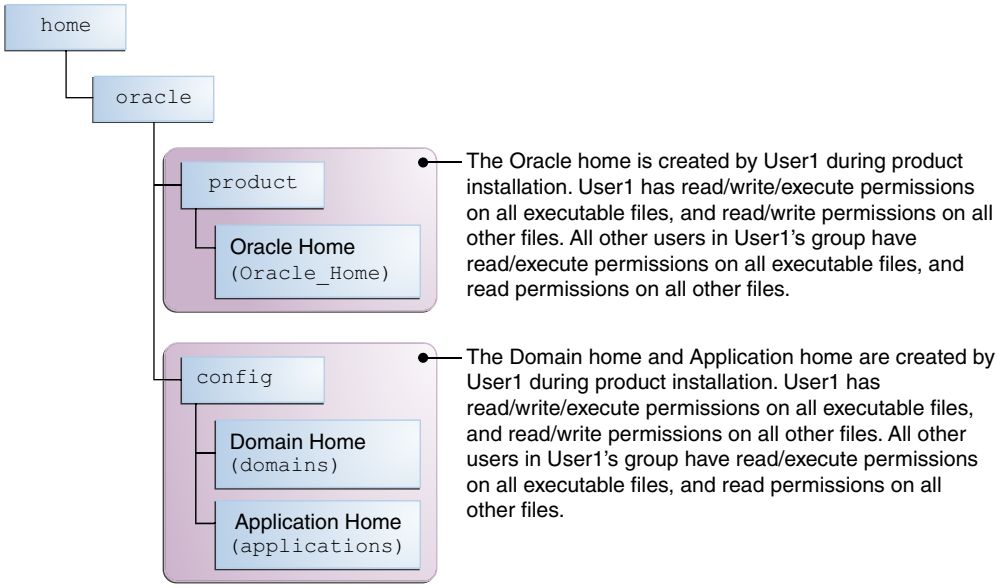
Consider the following examples:

- **Example 1: A Single User Installs the Software and Configures the Domain**

  This example explains the file permissions where the same user installs the software and configures the domain.

  To ensure proper permissions and privileges for all files, Oracle recommends that the same owner perform both tasks: install the Oracle Fusion Middleware product and configure the WebLogic Server domain by using the Configuration Wizard.

Figure 2-1 Directory Structure when a Single User Installs the Software and Configures the Domain

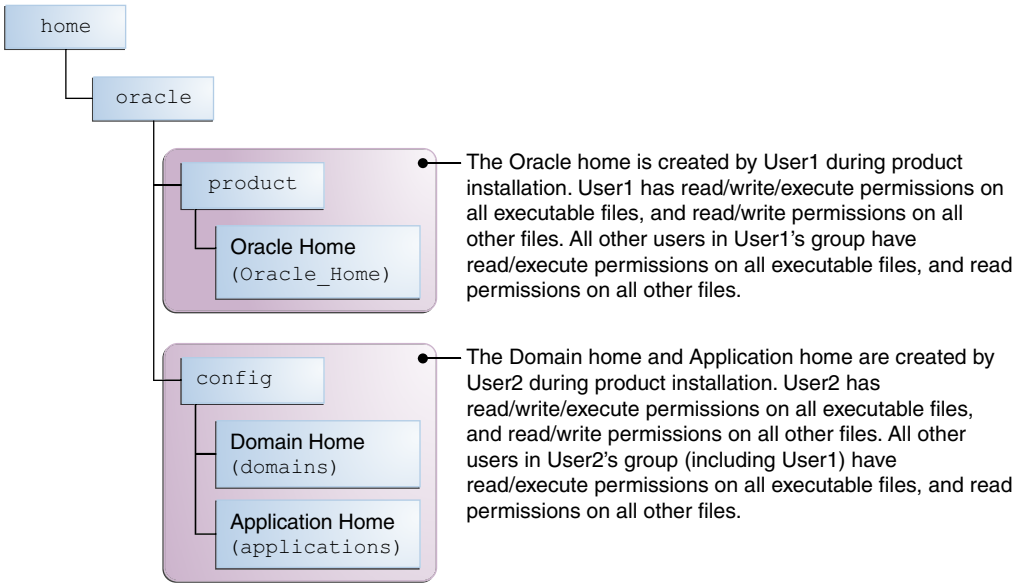


If the user who creates the domain is different than the user who installed the software, then both users must have the same privileges, as shown in the next example.

- **Example 2: The Oracle Home Directory and Domain are Created by Different Users**

  This example explains the file permissions where one user creates the Oracle home and another user configures the domain.

Figure 2-2 Directory Structure when Different Users Install the Software and Configure the Domain



> **Note:**
>
> Certain domain files do not have group permissions. For example, `cwallet.sso`.

Consider the following points before you run the installer:

- On UNIX operating systems, Oracle recommends that you set `umask` to `027` on your system before you install the software. This ensures that the file permissions are set properly during installation. Use the following command:

  ```
  umask 027
  ```

  You must enter this command in the same terminal window from which you plan to run the product installer.
- On UNIX operating systems, do not run the installation program as a `root` user. If you run the installer as a root user, the startup validation may fail and you cannot continue the installation.
- When you manage a product installation (for example, applying patches or starting managed Servers), use the same user ID that you used to install the product.
- On Windows operating systems, you must have administrative privileges to install the product. See Verifying the Installation User has Administrator Privileges on Windows Operating Systems.

Understanding Non-Default User Permissions on UNIX Operating Systems

Changing the default permissions setting reduces the security of the installation and possibly your system. Oracle does not recommend changing default permission settings.

If other users require access to particular files or executable, consider using the UNIX `sudo` command (or other similar command) in lieu of changing file permissions.

Refer to your UNIX operating system Administrator's Guide or contact your operating system vendor if you need further assistance.

Verifying that the Installation User has Administrator Privileges on Windows Operating Systems

To update the Windows Registry, you must have administrator privileges.

By default, users with the administrator privilege sign in to the system with regular privileges, but can request elevated permissions to perform administrative tasks.

To perform a task with elevated privileges:

1. Find the Command Prompt icon, either from the Start menu or the Windows icon in the lower-left corner.
2. Right-click **Command Prompt** and select **Run as administrator**.

   This opens a new command prompt window, and all actions performed in this window are done with administrator privileges.

> **Note:**
>
> If you have User Access Control enabled on your system, you may see an additional window asking you to confirm this action. Confirm and continue with this procedure.

3. Perform the desired task.

   For example, to start the product installer:

   For a jar file, enter:

   ```
   java –jar distribution_name.jar
   ```

   For an executable (`.exe`, `.bin`, or `.sh` file), enter:

   ```
   distribution_name.exe
   ```

About the Directories for Installation and Configuration

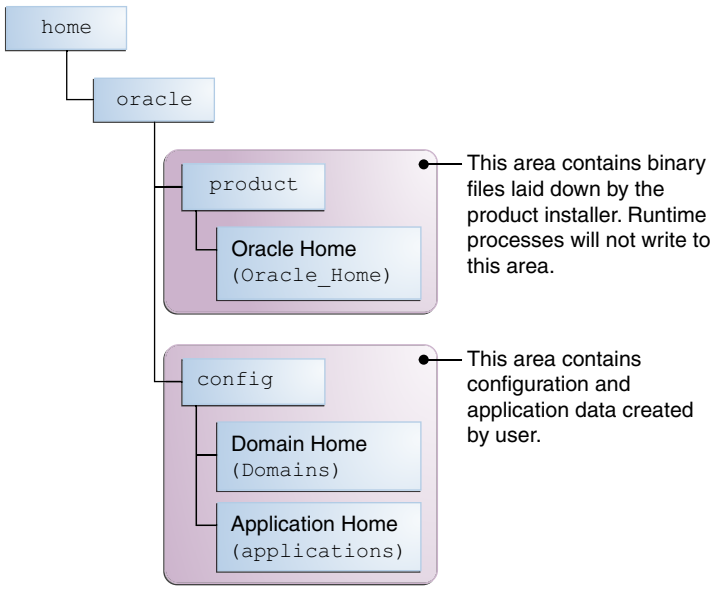
During the installation and domain configuration process, you must plan on providing the locations for these directories: Oracle home, Domain home, and the Application home.

About the Recommended Directory Structure

Oracle recommends specific locations for the Oracle Home, Domain Home, and Application Home.

Oracle recommends a directory structure similar to the one shown in Figure 2-3.

Figure 2-3 Recommended Oracle Fusion Middleware Directory Structure



A base location (Oracle base) should be established on your system (for example, `/home/oracle`). From this base location, create two separate branches, namely, the `product` directory and the `config` directory. The `product` directory should contain the product binary files and all

the Oracle home directories. The `config` directory should contain your domain and application data.

Oracle recommends that you do not keep your configuration data in the Oracle home directory; if you upgrade your product to another major release, you are required to create an Oracle home for binary files. You must also make sure that your configuration data exists in a location where the binary files in the Oracle home have access.

The `/home/oracle/product` (for the Oracle home) and `/home/oracle/config` (for the application and configuration data) directories are used in the examples throughout the documentation; be sure to replace these directories with the actual directories on your system.

About the Oracle Home Directory

When you install any Oracle Fusion Middleware product, you must use an Oracle home directory.

This directory is a repository for common files that are used by multiple Fusion Middleware products installed on the same machine. These files ensure that Fusion Middleware operates correctly on your system. They facilitate checking of cross-product dependencies during installation. For this reason, you can consider the Oracle home directory a *central support directory* for all Oracle Fusion Middleware products installed on your system.

Fusion Middleware documentation refers to the Oracle home directory as *ORACLE_HOME*.

Oracle Home Considerations

Keep the following in mind when you create the Oracle home directory and install the Oracle Fusion Middleware products:

- Do not include spaces in the name of your Oracle home directory; the installer displays an error message if your Oracle home directory path contains spaces.
- You can install only one instance of each Oracle Fusion Middleware product in a single Oracle home directory. If you need to maintain separate versions of a product on the same machine, each version must be in its own Oracle home directory.

  Although you can have several different products in a single Oracle home, only one version of each product can be in the Oracle home.

Multiple Home Directories

Although in most situations, a single Oracle home directory is sufficient, it is possible to create more than one Oracle home directory. For example, you need to maintain multiple Oracle home directories in the following situations:

- You prefer to maintain separate development and production environments, with a separate product stack for each. With two directories, you can update your development environment without modifying the production environment until you are ready to do so.
- You want to maintain two different versions of a Fusion Middleware product at the same time. For example, you want to install a new version of a product while keeping your existing version intact. In this case, you must install each product version in its own Oracle home directory.
- You need to install multiple products that are not compatible with each other. See Oracle Fusion Middleware Interoperability and Compatibility in *Understanding Interoperability and Compatibility* .

> **Note:**
>
> If you create more than one Oracle home directory, you must provide non-overlapping port ranges during the configuration phase for each product.

About the Domain Home Directory

The Domain home is the directory where domains that you configure are created.

The default Domain home location is *ORACLE_HOME*/user_projects/domains/*domain_name*.

> **Note:**
>
> Oracle strongly recommends that you do not use the default location. Put your Domain home *outside* of the Oracle home directory, for example, in /home/oracle/config/domains.

The config directory should contain domain and application data. Oracle recommends a separate domain directory so that new installs, patches, and other operations update the *ORACLE_HOME* only, *not* the domain configuration.

See About the Recommended Directory Structure for more on the recommended directory structure and locating your Domain home.

Fusion Middleware documentation refers to the Domain home directory as *DOMAIN_HOME* and includes all folders up to and including the domain name. For example, if you name your domain exampledomain and locate your domain data in the /home/oracle/config/domains directory, the documentation would use *DOMAIN_HOME* to refer to /home/oracle/config/domains/exampledomain.

About the Application Home Directory

The Application home is the directory where applications for domains you configure are created.

The default Application home location is *ORACLE_HOME*/user_projects/applications/*domain_name*. However, Oracle strongly recommends that you locate your Application home *outside* of the Oracle home directory; if you upgrade your product to another major release, you must create an Oracle home for binary files.

See About the Recommended Directory Structure for more on the recommended directory structure and locating your Application home.

Fusion Middleware documentation refers to the Application home directory as *APPLICATION_HOME* and includes all folders up to and including the domain name. For example, if you name your domain exampledomain and you locate your application data in the /home/oracle/config/applications directory, the documentation uses *APPLICATION_HOME* to refer to /home/oracle/config/applications/exampledomain.

Installing Multiple Products in the Same Domain

There are two methods to install and configure multiple products in one domain. This is also known as *extending* a domain.

- **Method 1.**

  Install and configure Product A, including creating the schemas and starting all servers in the domain to verify a successful domain configuration.

  This is the method used in all installation guides in the Fusion Middleware library. You can repeat this process for as many products as necessary. It allows you to validate one product at a time and add more products incrementally.

  To install Product B in the same domain as Product A:

  1. Stop all servers to prevent any updates to the domain while you add the new product.

     See Starting and Stopping Oracle Fusion Middleware in *Administering Oracle Fusion Middleware*.

  2. Follow the instructions in the installation guide for Product B, including creating the necessary schemas.

  3. Run the Configuration Wizard to configure the domain.

     During configuration, the Configuration Wizard automatically detects the components that have been installed and offers you the option to extend the existing Product A domain to include Product B.

- **Method 2.**

  Install all of the required products, then create the schemas for all of the products. After you create the schemas, configure the domain by using the necessary product templates, then start all the servers.

  This method of creating a multi-product domain may be slightly faster than Method 1; however, the installation guides in the Fusion Middleware library do not provide specific instructions for this method of domain creation.

See Also:

- To update WebLogic domains, see Updating WebLogic Domains in *Creating WebLogic Domains Using the Configuration Wizard*.
- For important information regarding the ability of Oracle Fusion Middleware products to function with previous versions of other Oracle Fusion Middleware, Oracle, or third-party products, see Oracle Fusion Middleware Interoperability and Compatibility in *Understanding Interoperability and Compatibility*.

Preparing for Shared Storage

Oracle Fusion Middleware allows you to configure multiple WebLogic Server domains from a single Oracle home. This allows you to install the Oracle home in a single location on a shared volume and reuse the Oracle home for multiple host installations.

If you plan to use shared storage in your environment, see Using Shared Storage in *High Availability Guide* for more information.

About JDK Requirements for an Oracle Fusion Middleware Installation

Most Fusion Middleware products are in `.jar` file format. These distributions do not include a JDK. To run a `.jar` distribution installer, you must have a certified JDK installed on your system.

Make sure that the JDK is installed *outside* of the Oracle home. If you install the JDK under the Oracle home, you may encounter problems when you try to perform tasks in the future. Oracle Universal Installer validates that the Oracle home directory is empty; the install does not progress until you specify an empty directory. Oracle recommends that you locate your JDK installation in the `/home/oracle/products/jdk` directory.

Platform-specific distributions have a `.bin` (for Linux operating systems) or `.exe` (for Windows operating systems) installer; in these cases, a platform-specific JDK is in the distribution and you do not need to install a JDK separately. However, you may need to upgrade this JDK to a more recent version, depending on the JDK versions that are certified.

Always verify the required JDK version by reviewing the certification information on the *Oracle Fusion Middleware Supported System Configurations* page for Oracle Fusion Middleware 14c (14.1.2.0.0).

To download the required JDK, navigate to the following URL and download the Java SE JDK:

http://www.oracle.com/technetwork/java/javase/downloads/index.html

About Database Requirements for an Oracle Fusion Middleware Installation

Many Oracle Fusion Middleware products require database schemas prior to configuration. If you do not already have a database where you can install these schemas, you must install and configure a certified database.

To find a certified database for your operating system, see the certification document for your release on the *Oracle Fusion Middleware Supported System Configurations* page on the Oracle Technology Network (OTN).

To make sure that your database is properly configured for schema creation, see *Repository Creation Utility Requirements* in the *Oracle Fusion Middleware System Requirements and Specifications* document.

After your database is properly configured, you use the Repository Creation Utility (RCU) to create product schemas in your database. This tool is available in the Oracle home for your Oracle Fusion Middleware product. See About the Repository Creation Utility in *Creating Schemas with the Repository Creation Utility*.

Obtaining the Product Distribution

You can obtain the Oracle Fusion Middleware Infrastructure and Oracle WebCenter Content distribution on *Technical Resources from Oracle*.

To prepare to install Oracle Fusion Middleware Infrastructure and Oracle WebCenter Content:

1. Enter `java -version` on the command line to verify that a certified JDK is installed on your system. For 14c (14.1.2.0.0), the certified JDK is 17.0.12 and later.

   See About JDK Requirements for an Oracle Fusion Middleware Installation.

2. Locate and download the Oracle Fusion Middleware Infrastructure and Oracle WebCenter Content software.

   See Obtaining Product Distributions in *Planning an Installation of Oracle Fusion Middleware*.

   To obtain the distribution for product evaluation, visit the Oracle Software Delivery Cloud page.

After preparing to install and configure the software, see Installing the Oracle WebCenter Content Software.

About Product Distributions

You create the initial Oracle WebCenter Content domain using the Oracle Fusion Middleware Infrastructure distribution, which contains both Oracle WebLogic Server software and Oracle Java Required Files (JRF) software.

Oracle JRF software consists of:

- Oracle Web Services Manager
- Oracle Application Development Framework (Oracle ADF)
- Oracle Enterprise Manager Fusion Middleware Control
- Repository Creation Utility (RCU)
- Other libraries and technologies required to support Oracle Fusion Middleware products

Prerequisites:

- Install Oracle Fusion Middleware Infrastructure. For more information about installing Oracle Fusion Middleware Infrastructure, see Installing the Infrastructure Software in the *Installing and Configuring the Oracle Fusion Middleware Infrastructure*.

> **Note:**
>
> If you want to access public internet cloud data sources, you must have a direct network connection as connections via proxy servers are not supported.

Verifying Digital Signature and Integrity of Installation Archive Files

Oracle digitally signs the installation archive files with Oracle certificates to ensure the integrity of the packages before you deploy them in your environments.

Use the Java utility `jarsigner` to verify the integrity of your installation archive files. You can verify the integrity of the installation archive files before you extract the installation files.

Quick Verification

To quickly verify the installation archive files, use the `jarsigner` command with the `-verify` option:

1. Go to the directory where you have downloaded the installation archive files.

2. Run this command to check your installation archive file:

```
jarsigner -verify installation_archive_file
```

For example, to check the Oracle Fusion Middleware Infrastructure archive:

```
jarsigner -verify fmw_14.1.2.0.0_infrastructure.jar


jar verified.
```

Detailed Certificate Information

If you want detailed certificate information, then use the `-verbose:summary` and `-certs` along with the `-verify` option.

1. Go to the directory where you have downloaded the installation archive files.
2. Run this command to check your installation archive file:

```
jarsigner -verify -verbose:summary -certs installation_archive_file
```

For example, to check the Oracle Fusion Middleware Infrastructure image:

```
jarsigner -verify -verbose:summary -certs fmw_14.1.2.0.0_infrastructure.jar
```

The output is similar to the following:

```
2237119 Fri Dec 6 07:02:30 UTC 2023 META-INF/MANIFEST.MF

      >>> Signer
      X.509, CN="Oracle America, Inc.", O="Oracle America, Inc.",
L=Redwood City, ST=California, C=US
      [
      Signature algorithm: SHA256withRSA, 3072-bit key
      [certificate is valid from 12/19/24 12:00 AM to 12/19/25 11:59 PM]
      X.509, CN=DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1,
O="DigiCert, Inc.", C=US
      [
      Signature algorithm: SHA384withRSA, 4096-bit key
      [certificate is valid from 4/29/24 12:00 AM to 4/28/36 11:59 PM]
      X.509, CN=DigiCert Trusted Root G4, O=DigiCert Inc, C=US
      [
      Signature algorithm: SHA384withRSA, 4096-bit key
      [trusted certificate]
      >>> TSA
      X.509, CN=DigiCert Timestamp 2024 - 2, O=DigiCert, C=US
      [
      Signature algorithm: SHA256withRSA, 4096-bit key
      [certificate is valid from 9/21/24 12:00 AM to 11/21/33 11:59 PM]
      X.509, CN=DigiCert Trusted G4 RSA4096 SHA256 TimeStamping CA,
O="DigiCert, Inc.", C=US
      [
      Signature algorithm: SHA256withRSA, 4096-bit key
      [certificate is valid from 3/23/24 12:00 AM to 3/22/37 11:59 PM]
```

```
      X.509, CN=DigiCert Trusted Root G4, O=DigiCert Inc, C=US
      [
      Signature algorithm: SHA384withRSA, 4096-bit key
      [certificate is valid from 8/1/24 12:00 AM to 11/9/31 11:59 PM]

       2237281 Fri Feb 17 07:02:32 UTC 2024 META-INF/ORACLE_C.SF (and 1
more)

      (Signature related entries)

            0 Fri Feb 17 05:41:24 UTC 2023 OPatch/ (and 1897 more)

      (Directory entries)

       2977 Tue Dec 20 08:02:16 UTC 2024 OPatch/README.txt (and 20199 more)

      [entry was signed on 2/17/24 7:02 AM]
      >>> Signer
      X.509, CN="Oracle America, Inc.", O="Oracle America, Inc.",
L=Redwood City, ST=California, C=US
      [
      Signature algorithm: SHA256withRSA, 3072-bit key
      [certificate is valid from 8/19/24 12:00 AM to 8/19/25 11:59 PM]
      X.509, CN=DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1,
O="DigiCert, Inc.", C=US
      [
      Signature algorithm: SHA384withRSA, 4096-bit key
      [certificate is valid from 4/29/24 12:00 AM to 4/28/36 11:59 PM]
      X.509, CN=DigiCert Trusted Root G4, O=DigiCert Inc, C=US
      [
      Signature algorithm: SHA384withRSA, 4096-bit key
      [trusted certificate]
      >>> TSA
      X.509, CN=DigiCert Timestamp 2024 - 2, O=DigiCert, C=US
      [
      Signature algorithm: SHA256withRSA, 4096-bit key
      [certificate is valid from 9/21/24 12:00 AM to 11/21/33 11:59 PM]
      X.509, CN=DigiCert Trusted G4 RSA4096 SHA256 TimeStamping CA,
O="DigiCert, Inc.", C=US
      [
      Signature algorithm: SHA256withRSA, 4096-bit key
      [certificate is valid from 3/23/24 12:00 AM to 3/22/37 11:59 PM]
      X.509, CN=DigiCert Trusted Root G4, O=DigiCert Inc, C=US
      [
      Signature algorithm: SHA384withRSA, 4096-bit key
      [certificate is valid from 8/1/24 12:00 AM to 11/9/31 11:59 PM]


  s = signature was verified
  m = entry is listed in manifest
  k = at least one certificate was found in keystore
  i = at least one certificate was found in identity scope

- Signed by "CN="Oracle America, Inc.", O="Oracle America, Inc.",
L=Redwood City, ST=California, C=US"
    Digest algorithm: SHA-256
```

```
    Signature algorithm: SHA256withRSA, 3072-bit key
  Timestamped by "CN=DigiCert Timestamp 2024 - 2, O=DigiCert, C=US" on Fri
Feb 17 07:02:33 UTC 2024
    Timestamp digest algorithm: SHA-256
    Timestamp signature algorithm: SHA256withRSA, 4096-bit key

jar verified.

The signer certificate will expire on 2025-12-19.
The timestamp will expire on 2031-11-09.
```

3

Installing the Oracle WebCenter Content Software

Follow the steps in this section to install the Oracle WebCenter Content software. Before beginning the installation, ensure that you have verified the prerequisites and completed all steps covered in Preparing to Install and Configure Oracle WebCenter Content.

Verifying the Installation Checklist

The installation process requires specific information.

Table 3-1 lists important items that you must know before, or decide during, Oracle WebCenter Content installation.

Table 3-1 Installation Checklist

Information	Example Value	Description
`JAVA_HOME`	`/home/Oracle/Java/jdk17.0.12`	Environment variable that points to the Java JDK home directory.
Database host	`examplehost.exampledomain`	Name and domain of the host where the database is running.
Database port	`1521`	Port number that the database listens on. The default Oracle database listen port is `1521`.
Database service name	`orcl.exampledomain`	Oracle databases require a unique service name. The default service name is `orcl`.
DBA username	`SYS`	Name of user with database administration privileges. The default DBA user on Oracle databases is `SYS`.
DBA password	`password`	Password of the user with database administration privileges.
`ORACLE_HOME`	`/home/Oracle/`*`product`*`/ORACLE_HOME`	Directory in which you will install your software. This directory will include Oracle Fusion Middleware Infrastructure and Oracle WebCenter Content, as needed.
WebLogic Server hostname	`examplehost.exampledomain`	Host name for Oracle WebLogic Server and Oracle WebCenter Content consoles.

Table 3-1 (Cont.) Installation Checklist

Information	Example Value	Description
Console port	**Note:** The default port values will vary depening on how you conifigured your domain. For a list of default values, see Port Numbers by Product and Component.	Port for Oracle WebCenter Content consoles.
DOMAIN_HOME	`/home/Oracle/config/domains/wcc_domain`	Location in which your domain data is stored.
APPLICATION_HOME	`/home/Oracle/config/applications/wcc_domain`	Location in which your application data is stored.

Table 3-1 (Cont.) Installation Checklist

Information	Example Value	Description
Administrator user name for your WebLogic domain	`weblogic`	Name of the user with Oracle WebLogic Server administration privileges. The default administrator user is `weblogic`.
Administrator user password	`password`	Password of the user with Oracle WebLogic Server administration privileges.
RCU	*`ORACLE_HOME`*`/oracle_common/bin`	Path to the Repository Creation Utility (RCU).
RCU schema prefix	`SHORT PRODUCT NAME`	Prefix for names of database schemas used by Oracle WebCenter Content.
RCU schema password	`password`	Password for the database schemas used by Oracle WebCenter Content.
Configuration utility	*`ORACLE_HOME`*`/oracle_common/common/bin`	Path to the Configuration Wizard for domain creation and configuration.

Starting the Installation Program

Before running the installation program, you must verify the JDK and prerequisite software is installed.

To start the installation program:

1. Sign in to the host system.
2. Change to the directory where you downloaded the installation program.
3. You must have installed the Oracle Fusion Middleware Infrastructure 14c (14.1.2.0.0). For instructions, see Installing the Infrastructure Software in *Installing and Configuring the Oracle Fusion Middleware Infrastructure*.
4. Start the installation program by running the `java` executable from the JDK directory. For example:
   - (UNIX) `/home/Oracle/Java/jdk17.0.12/bin/java -jar fmw_14.1.2.0.0_wcsites.jar`
   - (Windows) `C:\home\Oracle\Java\jdk17.0.12\bin\java -jar fmw_14.1.2.0.0_wcsites.jar`

> **Note:**
>
> You can also start the installer in silent mode using a saved response file instead of launching the installer screens. For more about silent or command line installation, see Using the Oracle Universal Installer in Silent Mode in *Installing Software with the Oracle Universal Installer*.

When the installation program appears, you are ready to begin the installation.

Navigating the Installation Screens

The installer shows a series of screens where you verify or enter information.

Table 3-2 lists the order in which installer screens appear. If you need additional help with an installation screen, click **Help**.

Table 3-2 Install Screens

Screen	Description
Installation Inventory Setup	On Linux or Unix operating systems, this screen opens if this is the first time you are installing any Oracle product on this host. Specify the location where you want to create your central inventory. Make sure that the operating system group name selected on this screen has write permissions to the central inventory location. See About the Oracle Central Inventory in *Installing Software with the Oracle Universal Installer*. This screen does not appear on Windows operating systems.
Welcome	Review the information to make sure that you have met all the prerequisites, then click **Next**.
Auto Updates	Select to skip automatic updates, select patches, or search for the latest software updates, including important security updates, through your My Oracle Support account.
Installation Location	Specify your Oracle home directory location. You can click **View** to verify and ensure that you are installing in the correct Oracle home.
Prerequisite Checks	This screen verifies that your system meets the minimum necessary requirements. To view the list of tasks that gets verified, select **View Successful Tasks**. To view log details, select **View Log**. If any prerequisite check fails, then an error message appears at the bottom of the screen. Fix the error and click **Rerun** to try again. To ignore the error or the warning message and continue with the installation, click **Skip** (not recommended).
Installation Summary	Use this screen to verify installation options you selected. If you want to save these options to a response file, click **Save Response File** and enter the response file location and name. The response file collects and stores all the information that you have entered, and enables you to perform a silent installation (from the command line) at a later time. Click **Install** to begin the installation.
Installation Progress	This screen shows the installation progress. When the progress bar reaches 100% complete, click **Finish** to dismiss the installer, or click **Next** to see a summary.
Installation Complete	This screen displays the Installation Location and the Feature Sets that are installed. Review this information and click **Finish** to close the installer.

Verifying the Installation

After you complete the installation, verify whether it was successful by completing a series of tasks.

Reviewing the Installation Log Files

Review the contents of the installation log files to make sure that the installer did not encounter any problems.

By default, the installer writes logs files to the *Oracle_Inventory_Location*/logs directory on Linux operating systems.

In case of Windows operating systems, the installer writes logs files to the *Oracle_Inventory_Location*\logs directory.

For a description of the log files and where to find them, see Installation Log Files in *Installing Software with the Oracle Universal Installer*.

Checking the Directory Structure

The contents of your installation vary based on the options that you selected during the installation.

See What Are the Key Oracle Fusion Middleware Directories? in *Understanding Oracle Fusion Middleware*.

Viewing the Contents of the Oracle Home

You can view the contents of the Oracle home directory by using the `viewInventory` script.

See Viewing the Contents of an Oracle Home in *Installing Software with the Oracle Universal Installer*.

4

Configuring WebCenter Content Domain

After you have installed WebCenter Content, you can configure the domain, which you can also extend for high availability.

The configuration steps presented here assume that you have completed the installation steps covered in:

- Preparing to Install and Configure Oracle WebCenter Content
- Installing the Oracle WebCenter Content Software

Refer to the following sections to create the database schemas, configure a WebLogic domain, and verify the configuration:

Creating the Database Schemas

Before you can configure a domain, you must install required schemas on a certified database for use with this release of Oracle Fusion Middleware.

> **Note:**
>
> As of Oracle Fusion Middleware 14c (14.1.2.0.0), new schemas are created with editions-based redefinition (EBR) views enabled by default. When EBR is enabled, the schema objects can be upgraded online to a future Fusion Middleware release without any downtime. For more information about using editions-based redefinition, see Using Edition-based Redefinition.

Installing and Configuring a Certified Database

Before you create the database schemas, you must install and configure a certified database, and verify that the database is up and running.

> **Note:**
>
> For an Autonomous Transaction Processing database (both Autonomous Transaction Processing-Dedicated (ATP-D) and Autonomous Transaction Processing Shared (ATP-S)), you must modify the wallet settings and set the environment variables as described in Settings to connect to Autonomous Transaction Processing Database, and apply patches on `ORACLE HOME` as described in Applying Patches on ORACLE HOME.

See About Database Requirements for an Oracle Fusion Middleware Installation.

Starting the Repository Creation Utility

Start the Repository Creation Utility (RCU) after you verify that a certified JDK is installed on your system.

To start the RCU:

1. Verify that a certified JDK already exists on your system by running `java -version` from the command line. For 14c (14.1.2.0.0), the certified JDK is 17.0.12 and later.

   See About JDK Requirements for an Oracle Fusion Middleware Installation.
2. Ensure that the `JAVA_HOME` environment variable is set to the location of the certified JDK.
3. Change to the following directory:
   - (UNIX) *ORACLE_HOME*`/oracle_common/bin`
   - (Windows) *ORACLE_HOME*`\oracle_common\bin`
4. Enter the following command:
   - (UNIX) `./rcu`
   - (Windows) `rcu.bat`

Navigating the Repository Creation Utility Screens to Create Schemas

Enter required information in the RCU screens to create the database schemas.

Introducing the RCU

The Welcome screen is the first screen that appears when you start the RCU.

Click **Next**.

Selecting a Method of Schema Creation

Use the Create Repository screen to select a method to create and load component schemas into the database.

On the Create Repository screen:

- If you have the necessary permissions and privileges to perform DBA activities on your database, select **System Load and Product Load**. This procedure assumes that you have SYSDBA privileges.
- If you do *not* have the necessary permissions or privileges to perform DBA activities in the database, you must select **Prepare Scripts for System Load** on this screen. This option generates a SQL script that you can give to your database administrator. See About System Load and Product Load in *Creating Schemas with the Repository Creation Utility*.
- If the DBA has already run the SQL script for System Load, select **Perform Product Load**.

> **Note:**
>
> For an Autonomous Transaction Processing database (both Autonomous Transaction Processing-Dedicated (ATP-D) and Autonomous Transaction Processing Shared (ATP-S)), you must create schemas as a `Normal` user, and though, you do not have full SYS or SYSDBA privileges on the database, you must select **System Load and Product Load**.

Providing Database Connection Details

On the Database Connection Details screen, provide the database connection details for the RCU to connect to your database.

If you are unsure of the service name for your database, you can obtain it from the `SERVICE_NAMES` parameter in the initialization parameter file of the database. If the initialization parameter 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.

To provide the database connection details:

1. On the Database Connection Details screen, provide the database connection details.

   For example:

   Database Type: `Oracle Database`
   Connection String Format: `Connection Parameters or Connection String`
   Connection String:
   `examplehost.exampledomain.com:1521:Orcl.exampledomain.com`
   Host Name: `examplehost.exampledomain.com`
   Port: `1521`
   Service Name: `Orcl.exampledomain.com`
   User Name: `sys`
   Password: `******`
   Role: `SYSDBA`

2. Click **Next** to proceed, then click **OK** in the dialog window that confirms a successful database connection.

For information about specifying connection credentials when connecting to an Oracle database, see Connection Credentials for Oracle Databases and Oracle Databases with Edition-Based Redefinition.

Specifying a Custom Prefix and Selecting Schemas

You must enter a custom prefix to group schemas together, then select schemas you need. You can select the required schema on the Select Components screen.

Select **Create new prefix**, specify a custom prefix, then select the **WebCenter Content** schema. This action automatically selects the schema dependencies.

> **Tip:**
>
> You must make a note of the custom prefix you choose to enter here; you will need this later on during the domain creation process.

> **Note:**
>
> If you install WebCenter Content only and select the **Oracle WebCenter Content Server - Complete** schema (but no other schemas), you must select the **Metadata Services** schema. You must select **Metadata Services** because WebCenter Content User Interface requires it.
>
> 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.

The schema Common Infrastructure Services is also created automatically. It enables you to retrieve information from RCU during domain configuration. This schema is grayed out; you cannot select or deselect it. For more details, see Understanding the Service Table Schema in *Creating Schemas with the Repository Creation Utility*.

The custom prefix logically groups these schemas together for use in this domain only; you must create a unique set of schemas for each domain because schema sharing across domains is not supported.

> **Tip:**
>
> For more details about custom prefixes, see Understanding Custom Prefixes in *Creating Schemas with the Repository Creation Utility*.
>
> To organize your schemas in a multi-domain environment, see Planning Your Schema Creation in *Creating Schemas with the Repository Creation Utility*.

Click **Next** to proceed, then click **OK** on the dialog window confirming that prerequisite checking for schema creation was successful.

Specifying Schema Passwords

On the Schema Passwords screen, specify how you want to set the schema passwords on your database, then enter and confirm your passwords.

> **Note:**
>
> For an Autonomous Transaction Processing database (both Autonomous Transaction Processing-Dedicated (ATP-D) and Autonomous Transaction Processing Shared (ATP-S)), the schema password must be minimum 12 characters, and must contain at least one uppercase, one lower case, and one number.

You must make a note of the passwords you set on this screen; you will need them later on during the domain creation process.

Click **Next**.

Completing Schema Creation

Navigate through the remaining RCU screens to complete schema creation.

On the Map Tablespaces screen, the Encrypt Tablespace check box appears *only* if you enabled Transparent Data Encryption (TDE) in the database (Oracle or Oracle EBR) when you start the RCU.

To complete schema creation:

1. On the Map Tablespaces screen, select **Encrypt Tablespace** if you want to encrypt all new tablespaces that the RCU creates.
2. In the Completion Summary screen, click **Close** to dismiss the RCU.

   For an Autonomous Transaction Processing Shared (ATP-S) database, in the **Map Tablespaces** screen you must override the default tablespaces and the temporary tablespaces, and also override the additional tablespaces, if applicable. See Map Tablespaces.

   If you encounter any issues when you create schemas on an Autonomous Transaction Processing database (both Autonomous Transaction Processing-Dedicated (ATP-D) and Autonomous Transaction Processing Shared (ATP-S)), see Troubleshooting Tips for Schema Creation on an Autonomous Transaction Processing Database in *Creating Schemas with the Repository Creation Utility* and Issues Related to Product Installation and Configuration on an Autonomous Database in *Release Notes for Oracle Fusion Middleware Infrastructure*.

Configuring the Domain

Use the Configuration Wizard to create and configure a domain.

For information on other methods to create domains, see Additional Tools for Creating, Extending, and Managing WebLogic Domains in *Creating WebLogic Domains Using the Configuration Wizard*.

Starting the Configuration Wizard

Start the Configuration Wizard to begin configuring a domain.

> **Note:**
>
> For an Autonomous Transaction Processing Shared (ATP-S) database, before you start the Configuration Wizard, you must set the `TNS_ADMIN` property using the following command:
>
> `export TNS_ADMIN=/<$ORACLE_HOME>/network/admin.`
>
> You must change `$ORACLE_HOME` to your Oracle Home location. For example: `export TNS_ADMIN=/users/test/network/admin`
>
> Where, `/users/test/` is the Oracle Home location.

To start the Configuration Wizard:

1. Change to the following directory:

   (UNIX) *`ORACLE_HOME`*`/oracle_common/common/bin`

   (Windows) *`ORACLE_HOME`*`\oracle_common\common\bin`

   where *`ORACLE_HOME`* is your 14c (14.1.2.0.0) Oracle home.
2. Enter the following command:

   (UNIX) `./config.sh`

   (Windows) `config.cmd`

Navigating the Configuration Wizard Screens to Create and Configure the Domain

Enter required information in the Configuration Wizard screens to create and configure the domain for the topology.

> **Note:**
>
> You can use this procedure to extend an existing domain. If your needs do not match the instructions in the procedure, be sure to make your selections accordingly, or see the supporting documentation for more details.

Selecting the Configuration Type and Domain Home Location

Use the Configuration Type screen to select a Domain home directory location, optimally outside the Oracle home directory.

Oracle recommends that you locate your Domain home in accordance with the directory structure in What Are the Key Oracle Fusion Middleware Directories? in *Understanding Oracle*

Fusion Middleware, where the Domain home is located outside the Oracle home directory. This directory structure helps avoid issues when you need to upgrade or reinstall software.

To specify the Domain type and Domain home directory:

1. On the Configuration Type screen, select **Create a new domain**.
2. In the Domain Location field, specify your Domain home directory.

For more details about this screen, see Configuration Type in *Creating WebLogic Domains Using the Configuration Wizard*.

Selecting Configuration Templates for Oracle WebCenter Content

On the Templates screen, make sure **Create Domain Using Product Templates** is selected, then select the following templates:

- **Oracle Universal Content Management - Inbound Refinery - 14.1.2.0.0[wccontent]**
- **Oracle Universal Content Management - Content Server - 14.1.2.0.0 [wccontent]**

  Selecting this template automatically selects the following as dependencies:

  – Oracle Enterprise Manager - 14.1.2.0.0 [em]
  – Oracle JRF - 14.1.2.0.0 [oracle_common]
  – WebLogic Coherence Cluster Extension - 14.1.2.0.0 [wlserver]
- **Oracle WebCenter Enterprise Capture - 14.1.2.0.0 [wccapture]**
- **Oracle WebCenter Content - Web UI - 14.1.2.0.0 [wccontent]**
- **Oracle WebCenter Content: Imaging 14.1.2.0.0 [wcimaging]**

> **Tip:**
>
> For more details about options on this screen, see Templates in *Creating WebLogic Domains Using the Configuration Wizard*.

Configuring High Availability Options

Use this screen to configure service migration and persistence settings that affect high availability.

This screen appears for the first time when you create a cluster that uses automatic service migration, persistent stores, or both, and all subsequent clusters that are added to the domain by using the Configuration Wizard, automatically apply the selected HA options.

Enable Automatic Service Migration

Select **Enable Automatic Service Migration** to enable pinned services to migrate automatically to a healthy Managed Server for failover. It configures migratable target definitions that are required for automatic service migration and the cluster leasing. Choose one of these cluster leasing options:

- Database Leasing - Managed Servers use a table on a valid JDBC System Resource for leasing. Requires that the Automatic Migration data source have a valid JDBC System Resource. If you select this option, the Migration Basis is configured to Database and the Data Source for Automatic Migration is also automatically configured by the Configuration

Wizard. If you have a high availability database, such as Oracle RAC, to manage leasing information, configure the database for server migration.

- Consensus Leasing - Managed Servers maintain leasing information in-memory. You use Node Manager to control Managed Servers in a cluster. (All servers that are migratable, or which could host a migratable target, must have a Node Manager associated with them.) If you select this option, the Migration Basis is configured to Consensus by the Configuration Wizard.

See Leasing for more information on leasing.

See Service Migration for more information on Automatic Service Migration.

JTA Transaction Log Persistence

This section has two options: **Default Persistent Store** and **JDBC TLog Store**.

- Default Persistent Store - Configures the JTA Transaction Log store of the servers in the default file store.
- JDBC TLog Store - Configures the JTA Transaction Log store of the servers in JDBC stores.

Oracle recommends that you select **JDBC TLog Store**. When you complete the configuration, you have a cluster where JDBC persistent stores are set up for Transaction logs.

For more details on persistent and TLOG stores, see the following topics in *Developing JTA Applications for Oracle WebLogic Server*:

- Using the Default Persistent Store
- Using a JDBC TLOG Store

JMS Server Persistence

A persistent **JMS store** is a physical repository for storing persistent message data and durable subscribers. It can be either a disk-based **file store** or a JDBC-accessible database. You can use a **JMS file store** for paging of messages to disk when memory is exhausted.

- JMS File Store - Configures a component to use JMS File Stores. If you select this option, you can choose the **File Store** option in the Advanced Configuration Screen to change the settings, if required. In the File Stores screen, you can set file store names, directories, and synchronous write policies.
- JMS JDBC Store - Configures a component to use JDBC stores for all its JMS servers. When you complete the configuration, you have a cluster and JDBC persistent stores are configured for the JMS servers.

Selecting the Application Home Location

Use the Application Location screen to select the location to store applications associated with your domain, also known as the *Application home* directory.

Oracle recommends that you locate your Application home in accordance with the directory structure in What Are the Key Oracle Fusion Middleware Directories? in *Understanding Oracle Fusion Middleware*, where the Application home is located outside the Oracle home directory. This directory structure helps avoid issues when you need to upgrade or re-install your software.

For more about the Application home directory, see About the Application Home Directory.

For more information about this screen, see Application Location in *Creating WebLogic Domains Using the Configuration Wizard*.

Configuring the Administrator Account

Use the Administrator Account screen to specify the username and password for the default WebLogic Administrator account for the domain.

Oracle recommends that you make a note of the username and password that you enter on this screen; you need these credentials later to boot and connect to the domain's Administration Server.

Specifying the Domain Mode and JDK

Use the Domain Mode and JDK screen to specify the domain mode and Java Development Kit (JDK) for your production environment.

On the Domain Mode and JDK screen:

- Select **Production** in the **Domain Mode** field.

> **Note:**
>
> As of WebLogic Server 14.1.2.0.0, when you select **Production** mode, WebLogic Server automatically sets some of the security configurations of **Secured Production** to more secure values. However, there are certain security configurations (such as SSL/TLS) that require manual configuration. See Using Secured Production Mode in *Administering Security for Oracle WebLogic Server*.
>
> If you want to disable the more secure default settings, then you may select **Disable Secure Mode**. This will enable the non-SSL listen ports.
>
> If you want to retain the more secure default settings of **Secured Production** mode in general, but want to change which ports (listen ports, SSL listen ports, or administration ports) will be enabled by default in your domain, then you may:
>
> – Leave **Disable Secure Mode** unselected, and
>
> – Change the default port selections under **Enable or Disable Default Ports for Your Domain**
>
> For more information, see Understand How Domain Mode Affects the Default Security Configuration in *Securing a Production Environment for Oracle WebLogic Server*.

- Select the **Oracle HotSpot JDK** in the **JDK** field.

For more information about this screen, see Domain Mode and JDK in *Creating WebLogic Domains Using the Configuration Wizard*.

Specifying JDBC Data Sources

Use this screen to specify JDBC Data Sources.

If you use a DB2 database, you must check system requirements before you select a DB2 driver. See the document *Oracle Fusion Middleware System Requirements and Specifications*.

1. Select the default Data Source, mds-WCCUIMDSREPO.

2. Enter values for DBMS/Service, Host Name, Port and Password and Username.

> **Note:**
>
> For an Autonomous Transaction Processing database, (both Autonomous Transaction Processing - Dedicated and Autonomous Transaction Processing-Shared), specify the connection credentials using only the **Connection URL String** option, and enter the connect string in the following format:
>
> `jdbc:oracle:thin:@TNS_alias?TNS_ADMIN=<path of the wallet files, ojdbc.properties, and tnsnames.ora>`
>
> In the connect string, you must pass `TNS_alias` as the database name found in `tnsnames.ora`, and `TNS_ADMIN` property to the location of the wallet files, `ojdbc.properties`, and `tnsnames.ora`.
>
> Example connect string for Autonomous Transaction Processing - Dedicated database:
>
> `jdbc:oracle:thin:@dbname_tp?TNS_ADMIN=/users/test/wallet_dbname/`
>
> Example connect string for Autonomous Transaction Processing-Shared database:
>
> `jdbc:oracle:thin:@dbname_tp?TNS_ADMIN=/users/test/wallet_dbname/`

3. Click **Next**.

Testing the JDBC Data Source

Use this screen to test the data source connections you configured in the previous screens.

> **Note:**
>
> To test database connections, the database you are connecting to must be running. If you don't want to test the connections at this time, do not select any data sources and click **Next** to continue.

A green check mark in the Status column indicates a successful test. If you encounter any issues, see the error message in the Connection Result Log section of the screen, fix the problem, then try to test the connection again.

To test the data source:

1. Select the check box next to the data source you want to test.
2. Select **Test Selected Connections**.
3. If the test is successful, then click **Next**. If it fails, click **Back**, correct the details and retest it.

Specifying the Database Configuration Type

Use the Database Configuration type screen to specify details about the database and database schema.

On the Database Configuration type screen, select **RCU Data**. This option instructs the Configuration Wizard to connect to the database and Service Table (STB) schema to automatically retrieve schema information for schemas needed to configure the domain.

> **Note:**
>
> If you select **Manual Configuration** on this screen, you must manually fill in parameters for your schema on the next screen.
>
> For an Autonomous Transaction Processing database, (both Autonomous Transaction Processing-Dedicated (ATP-D) and Autonomous Transaction Processing Shared (ATP-S)), you must select only the **RCU Data** option.

After selecting **RCU Data**, specify details in the following fields:

Field	Description
Host Name	Enter the name of the server hosting the database. Example: `examplehost.exampledomain.com`
DBMS/Service	Enter the database DBMS name, or service name if you selected a service type driver. Example: `orcl.exampledomain.com`
Port	Enter the port number on which the database listens. Example: `1521`
Schema Owner Schema Password	Enter the username and password for connecting to the database's Service Table schema. This is the schema username and password entered for the Service Table component on the Schema Passwords screen in the RCU (see Specifying Schema Passwords). The default username is *`prefix`*`_STB`, where *`prefix`* is the custom prefix that you defined in the RCU.

For an Autonomous Transaction Processing database (both Autonomous Transaction Processing-Dedicated (ATP-D) and Autonomous Transaction Processing Shared (ATP-S)), specify the connection credentials using only the **Connection URL String** option, and enter the connect string in the following format described in Connection Credentials for an Autonomous Transaction Processing Database.

Click **Get RCU Configuration** when you finish specifying the database connection information. The following output in the Connection Result Log indicates that the operation succeeded:

```
Connecting to the database server...OK
Retrieving schema data from database server...OK
Binding local schema components with retrieved data...OK

Successfully Done.
```

For more information about the schema installed when the RCU is run, see About the Service Table Schema in *Creating Schemas with the Repository Creation Utility*.

See Database Configuration Type in *Creating WebLogic Domains Using the Configuration Wizard* .

Specifying JDBC Component Schema Information

Use the JDBC Component Schema screen to verify or specify details about the database schemas.

Verify that the values populated on the JDBC Component Schema screen are correct for all schemas. If you selected **RCU Data** on the previous screen, the schema table should already be populated appropriately.

For an Autonomous Transaction Processing database (both Autonomous Transaction Processing-Dedicated (ATP-D) and Autonomous Transaction Processing Shared (ATP-S)), specify the connection credentials using only the **Connection URL String** option, and enter the connect string in the following format:

```
@TNS_alias?TNS_ADMIN=<path of the wallet files, ojdbc.properties, and
tnsnames.ora>
```

In the connect string, you must pass `TNS_alias` as the database service name found in `tnsnames.ora`, and `TNS_ADMIN` property to the location of the wallet files, `ojdbc.properties`, and `tnsnames.ora`.

Example connect string for Autonomous Transaction Processing-Dedicated (ATP-D) database:

```
@dbname_tp?TNS_ADMIN=/users/test/wallet_dbname/
```

Example connect string for Autonomous Transaction Processing Shared (ATP-S) database:

```
@dbname_tp?TNS_ADMIN=/users/test/wallet_dbname/
```

For high availability environments, see the following sections in *High Availability Guide* for additional information on configuring data sources for Oracle RAC databases:

- Configuring Active GridLink Data Sources with Oracle RAC
- Configuring Multi Data Sources

See JDBC Component Schema in *Creating WebLogic Domains Using the Configuration Wizard* for more details about this screen.

Testing the JDBC Connections

Use the JDBC Component Schema Test screen to test the data source connections.

A green check mark in the Status column indicates a successful test. If you encounter any issues, see the error message in the Connection Result Log section of the screen, fix the problem, then try to test the connection again.

By default, the schema password for each schema component is the password you specified while creating your schemas.

For more information about this screen, see JDBC Component Schema Test in *Creating WebLogic Domains Using the Configuration Wizard*.

Entering Credentials

Use the Credentials screen to set credentials for each key in the domain.

The Store Name column shows the credential store associated with each key.

(Optional) You can click **Add** to enter additional key credentials.

1. Enter the User Name to use for the key.
2. Enter the Password to use for the key.
3. Select **Next**.

Selecting Advanced Configuration

Use the Advanced Configuration screen to complete the domain configuration.

On the Advanced Configuration screen, select:

- Administration Server

  Required to properly configure the listen address of the Administration Server.
- Node Manager

  Required to configure Node Manager.
- Topology

  Required to configure the WebCenter Content Managed Server.

Optionally, select other available options as required for your desired installation environment. The steps in this guide describe a standard installation topology, but you may choose to follow a different path. If your installation requirements extend to additional options outside the scope of this guide, you may be presented with additional screens to configure those options. For information about all Configuration Wizard screens, see Configuration Wizard Screens in *Creating WebLogic Domains Using the Configuration Wizard*.

Configuring the Administration Server Listen Address

Use the Administration Server screen to select the Listen Address and configure the Administration Server ports.

> **Note:**
>
> The default port values will vary depening on how you conifigured your domain. The Enable SSL Listen Port is enabled by default, but the default values may change. For a list of default values, see Port Numbers by Product and Component.

1. Provide a name for the Administration Server. The name field must not be null or empty and cannot contain any special characters.
2. Select the drop-down list next to **Listen Address** and select the IP address of the host where the Administration Server will reside or use the system name or DNS name that maps to a single IP address. Do *not* use `All Local Addresses`.

3. Verify the port settings. When the domain type is set to Production, then the **Enable SSL Listen Port** option is enabled by default. Do *not* specify any server groups for the Administration Server.

> **Note:**
>
> You can change the port values as needed, but **they must be unique**. If the same port numbers are used for different ports, you will not be able to navigate to the next step in the Configuration Wizard.

For more information, see Specifying the Listen Address in *Creating WebLogic Domains Using the Configuration Wizard*.

> **Note:**
>
> Use a browser to access Internet Protocol Version 6 (IPv6) URLs. You must enter the Global IPv6 address to create a domain and access URLs. (You should not use the local IPv6 address.)

Configuring Node Manager

Use the Node Manager screen to select the type of Node Manager you want to configure, along with the Node Manager credentials.

Select **Per Domain Default Location** as the Node Manager type, then specify Node Manager credentials.

For more information about this screen, see Node Manager in *Creating WebLogic Domains Using the Configuration Wizard*.

For more information about Node Manager types, see About Node Manager in *Administering Node Manager for Oracle WebLogic Server*.

Configuring Managed Servers for Oracle WebCenter Content

You create and configure new Managed Servers on the Managed Servers Screen.

You create two Managed Servers for each component, with the exception of Inbound Refinery.

1. In the Listen Address drop-down list, select the IP address of the host on that the Managed Servers will reside on or use the system name or DNS name that maps to a single IP address. Do not use **All Local Addresses**.
2. Verify your port selections. If you selected Production mode with Secure Mode enabled, **Enable SSL Port** is selected by default. The default port will be auto-incremented so that the ports do not conflict with any additional managed servers you add. This is true for Listen Ports and Administration Ports. You can edit any and all port values based on your configuration and machines being used. For a list of port numbers for your components, see Port Numbers by Product and Component.

> **Note:**
>
> You can change the port values as needed, but they must be unique. If the same port numbers are used for different ports, you will receive a port conflict error and you will not be able to start the server.

Oracle recommends that you enable SSL ports for added security. If, however, you want to change the port setting to use the less secure Listen Port, then disable the Enable SSL Port and check the **Enable Listen Port** option.

3. Leave the Server Groups settings as they appear; the Configuration Wizard assigns the correct server group automatically. A server group ensures that the correct services target Managed Servers you are creating.

   Server groups target Fusion Middleware applications and services to one or more servers by mapping defined application service groups to each defined server group. You can map a given application service group to multiple server groups if needed. Any application services that map to a certain server group are automatically targeted to all servers assigned to that group. For more information about server groups, see Application Service Groups, Server Groups, and Application Service Mappings in *Domain Template Reference*.

4. Click **Add** and repeat this process to create a second Managed Server for each component except for Inbound Refinery. For example, `cpt_server_2`.

   You must configure a second Managed Server to configure the standard topology for high availability. If you are not creating a highly available environment, then this step is optional.

   For more about the high availability standard topology, see Understanding the Fusion Middleware Standard HA Topology in *High Availability Guide*.

   For more information about the next steps to prepare for high availability after your domain is configured, see Preparing Your Environment for High Availability.

Examples and procedures in the rest of this document refer to these server names; if you choose different names be sure to replace them as needed.

> **Tip:**
>
> For more about options on this screen, see Managed Servers in *Creating WebLogic Domains Using the Configuration Wizard*.

Configuring a Cluster for WebCenter Content

Use the Clusters screen to create a new cluster.

On the Clusters screen:

1. Click **Add**.
2. Specify `SOA_cluster1` in the Cluster Name field.
3. Leave the Cluster Address field blank.

Repeat the preceding steps to create three more clusters: `cpt_cluster1`, `ibr_cluster1`, and `wccui_cluster1`.

By default, server instances in a cluster communicate with one another using unicast. If you want to change your cluster communications to use multicast, see Considerations for Choosing Unicast or Multicast in *Administering Clusters for Oracle WebLogic Server*.

For more information about this screen, see Clusters in *Creating WebLogic Domains Using the Configuration Wizard*.

Defining Server Templates

If you are creating dynamic clusters for a high availability setup, use the Server Templates screen to define one or more server templates for the domain.

To add Server Templates:

> **Note:**
>
> The default port values will vary depening on how you conifigured your domain. The Enable SSL Listen Port is enabled by default, but the default values may change. For a list of default values, see Port Numbers by Product and Component.

1. Click **Add** to create `new_ServerTemplate_1`. The server template name will increment automatically when an additional server template is added (`new_ServerTemplate_2`).
2. For Secure Production Mode, verify that the **Enable SSL Port** option is selected. The default SSL Listen Port does not increment automatically when a new server template is added. You can change the default to Enable Listen Port, but Oracle recommends that retain the default to enable SSL. Enabling Listen Port disables SSL Listen Port.

   > **Note:**
   >
   > You can change the port values as needed using an integer in the range of 1 and 65535, but they must be unique. If the same port numbers are used for different ports, you will receive a port conflict error and you will not be able to start the server.

3. The Administration Port does not increment when an additional server template is added.

   > **Note:**
   >
   > If the Listen ports are disabled, then instead of seeing a number you will see `Disabled`.

For steps to create a dynamic cluster for a high availability setup, see Using Dynamic Clusters in *High Availability Guide*.

Configuring Dynamic Servers

If you are creating dynamic clusters for a high availability setup, use the Dynamic Servers screen to configure the dynamic servers.

If you are *not* configuring a dynamic cluster, click **Next** to continue configuring the domain.

> **Note:**
>
> When you create dynamic clusters, keep in mind that after you assign the **Machine Name Match Expression**, you do not need to create machines for your dynamic cluster.

To create a dynamic cluster for a high availability setup, see Using Dynamic Clusters in *High Availability Guide*.

Assigning WebCenter Content Managed Servers to the Cluster

Use the Assign Servers to Clusters screen to assign Managed Servers to a new *configured cluster*. A configured cluster is a cluster you configure manually. You do not use this screen if you are configuring a *dynamic cluster*, a cluster that contains one or more generated server instances that are based on a server template.

For more on configured cluster and dynamic cluster terms, see About Dynamic Clusters in *Understanding Oracle WebLogic Server*.

On the Assign Servers to Clusters screen:

1. In the Clusters pane, select the cluster to which you want to assign the Managed Servers; in this case, `wcc_cluster_1`.
2. In the Servers pane, assign `wcc_server_1` to `wcc_cluster_1` by doing one of the following:
   - Click once on `wcc_server_1` to select it, then click the right arrow to move it beneath the selected cluster (`wcc_cluster_1`) in the Clusters pane.
   - Double-click on `wcc_server_1` to move it beneath the selected cluster (`wcc_cluster_1`) in the Clusters pane.
3. Repeat to assign `wcc_server_2` to `wcc_cluster_1`.

The following image shows a generic example of the Clusters pane after Managed Servers are assigned to clusters.
For more information about this screen, see Assign Servers to Clusters in *Creating WebLogic Domains Using the Configuration Wizard*.

Configuring Coherence Clusters

Use the Coherence Clusters screen to configure the Coherence cluster.

Leave the default port number as the Coherence cluster listen port. After configuration, the Coherence cluster is automatically added to the domain.

> **Note:**
>
> Setting the unicast listen port to `0` creates an offset for the Managed Server port numbers. The offset is `5000`, meaning the maximum allowed value that you can assign to a Managed Server port number is `60535`, instead of `65535`.

For Coherence licensing information, see Oracle Coherence Products in *Licensing Information*.

Creating a New WebCenter Content Machine

Use the Machines screen to create new machines in the domain. A machine is required so that Node Manager can start and stop servers.

If you plan to create a high availability environment and know the list of machines your target topology requires, you can follow the instructions in this section to create all the machines at this time. For more about scale out steps, see Optional Scale Out Procedure in *High Availability Guide*.

To create a new WebCenter Content machine so that Node Manager can start and stop servers:

1. Select the Machine tab (for Windows) or the UNIX Machine tab (for UNIX), then click **Add** to create a new machine.
2. In the Name field, specify a machine name, such as `wcc_machine_1`.
3. In the Node Manager Listen Address field, select the IP address of the machine in which the Managed Servers are being configured.

   You must select a specific interface and not `localhost`. This allows Coherence cluster addresses to be dynamically calculated.
4. Verify the port in the Node Manager Listen Port field.
5. Repeat these steps to add more machines, if required.

> **Note:**
>
> If you are extending an existing domain, you can assign servers to any existing machine. It is not necessary to create a new machine unless your situation requires it.

For more information about this screen, see Machines in *Creating WebLogic Domains Using the Configuration Wizard*.

Assigning Servers to WebCenter Content Machines

Use the Assign Servers to Machines screen to assign the Administration Server and Managed Servers to the new machine you just created.

On the Assign Servers to Machines screen:

1. In the Machines pane, select the machine to which you want to assign the servers; in this case, `wcc_machine_1`.
2. In the Servers pane, assign `AdminServer` to `wcc_machine_1` by doing one of the following:
   - Click once on `AdminServer` to select it, then click the right arrow to move it beneath the selected machine (`wcc_machine_1`) in the Machines pane.
   - Double-click on `AdminServer` to move it beneath the selected machine (`wcc_machine_1`) in the Machines pane.
3. Repeat these steps to assign all Managed Servers to their respective machines.

For more information about this screen, see Assign Servers to Machines in *Creating WebLogic Domains Using the Configuration Wizard*.

Reviewing Your Configuration Specifications and Configuring the Domain

The Configuration Summary screen shows detailed configuration information for the domain you are about to create.

Review each item on the screen and verify that the information is correct. To make any changes, go back to a screen by clicking the **Back** button or selecting the screen in the navigation pane. Domain creation does not start until you click **Create**.

For more details about options on this screen, see Configuration Summary in *Creating WebLogic Domains Using the Configuration Wizard*.

Writing Down Your Domain Home and Administration Server URL

The End of Configuration screen shows information about the domain you just configured.

Make a note of the following items because you need them later:

- Domain Location
- Administration Server URL

You need the domain location to access scripts that start Node Manager and Administration Server, and you need the URL to access the Administration Server.

Click **Finish** to dismiss the Configuration Wizard.

Starting the Servers

After configuration is complete, start Node Manager, then the WebLogic Administration Server and Managed Servers.

> **Note:**
>
> Depending on your existing security settings, you may need to perform additional configuration before you can start and manage a domain with secured production mode enabled. Specifically, you will need to add additional parameters when starting the Administration and Managed Servers. For more information, see Using Secured Production Mode *Administering Security for Oracle WebLogic Server*.

For more information on additional tools you can use to manage your domain, see Overview of Oracle Fusion Middleware Administration Tools in *Administering Oracle Fusion Middleware*.

Starting Node Manager

To start the per-domain Node Manager:

1.
   - (UNIX) Go to the `DOMAIN_HOME/bin` directory.
   - (Windows) Go to the `DOMAIN_HOME\bin` directory.
2. Enter the following command:

- (UNIX) Using `nohup` and `nm.out` as an example output file:

  ```
  nohup ./startNodeManager.sh > LOG_DIR/nm.out&
  ```

  where *`LOG_DIR`* is the location of directory in which you want to store the log files.

- (Windows) `startNodeManager.cmd`

> **Note:**
>
> On Windows operating systems, Oracle recommends that you configure Node Manager to run as a startup service. This allows Node Manager to start up automatically each time the system is restarted.
>
> See Running Node Manager as a Startup Service in *Administering Node Manager for Oracle WebLogic Server*.

Starting the Administration Server

The procedures in this section describe how to start the Administration Server using the WLST command line or a script. You can also use the Oracle Fusion Middleware Control and the Oracle WebLogic Server Remote Console. See Starting and Stopping Administration and Managed Servers and Node Manager in *Administering Oracle Fusion Middleware.*

To start the Administration Server:

> **Note:**
>
> When using secured production mode, you must provide additional parameters to start the Administration Server. See Connecting to the Administration Server using WLST in *Administering Security for Oracle WebLogic Server*.

1. **(Optional)** When using **Production Mode**, you can create a *boot.properties* file before starting the Administration Server and provide necessary permissions. This file can be created to bypass the need to provide a username and password when starting the Administration Server. For more information, see Creating a Boot Identity File for an Administration Server in *Administering Server Startup and Shutdown for Oracle WebLogic Server*.
2. Go to the *`DOMAIN_HOME`*`/bin` directory.
3. Enter the following command:

   - (UNIX)

     ```
     ./startWebLogic.sh
     ```

   - (Windows)

     ```
     startWebLogic.cmd
     ```

   If you selected **Production Mode** on the Domain Mode and JDK screen when you created the domain, and you did not create the optional *boot.propeties* file, you see a prompt for the Administrator user login credentials as provided on the Administrator Account screen.

4. Open a browser and verify that the Administration Server is up and running. The default port values will vary depening on how you conifigured your domain. The Enable SSL Listen Port is enabled by default, but the default values may change. For a list of default values, see Port Numbers by Product and Component.

   ```
   https://<Host_Name>:<port>
   ```

5. Verify that all servers in the domain have unique port values. From the WebLogic Remote Console, you can review the **Local Administration Port Override** fields for each managed server and verify that each has a unique value. If one or more ports is using the same value, then you must change them before starting the managed servers. For more information about changing port values, see Connect to an Administration Server in the Oracle WebLogic Remote Console.

> **Note:**
>
> The WebLogic Server Administration Console has been removed. For comparable functionality, you should use the WebLogic Remote Console. For more information, see Oracle WebLogic Remote Console.

Starting the Managed Servers

To start a WebLogic Managed Server that is not set to secure product mode, you can use the `startManagedWebLogic` script:

- (UNIX) *`NEW_DOMAIN_HOME`*`/bin/startManagedWebLogic.sh` *`managed_server_name`*
- (Windows) *`NEW_DOMAIN_HOME`*`\bin\startManagedWebLogic.cmd` *`managed_server_name`*

> **Note:**
>
> When using secured production mode, you must provide additional parameters to start the Managed Servers. See Starting Managed Servers using a Start Script in *Administering Security for Oracle WebLogic Server*.

Oracle WebCenter Content Managed Server Locations (URLs)

After you start the Managed Servers, use this topic to refer to Oracle WebCenter Content Managed Server locations.

Server	URL
WebCenter Content	`http://`*`hostname`*`:`*`wcc-server-port`*`/cs`
WebCenter Content User Interface	`http://`*`hostname`*`:`*`wccui-server-port`*`/wcc`
Inbound Refinery	`http://`*`hostname`*`:`*`ibr-server-port`*`/ibr`
Capture	`http://`*`hostname`*`:`*`cpt-server-port`*`/`
WebCenter Content: Imaging	`http://hostname:imaging-server-port/imaging`

Verifying the Configuration

After completing all configuration steps, you can perform additional steps to verify that your domain is properly configured.

To verify that the domain is configured properly, see Performing Additional Domain Configuration Tasks.

Configuring Inbound Refinery Settings (Single Node)

After you start the Inbound Refinery Managed Servers, configure the settings on the post-installation configuration screen. In most cases, you can accept the default settings.

To configure the settings:

1. Access the Inbound Refinery post-installation configuration screen at the following URL:

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

2. Review the settings. See Inbound Refinery Configuration Page for a description of each field.
3. Click **Submit**.
4. Restart the Inbound Refinery Managed Server, using the WebLogic Server Administration Console.

Inbound Refinery Configuration Page

Use descriptions of Inbound Refinery configuration page fields as you complete configuration steps in Configuring Inbound Refinery Settings (Single Node).

The following table describes Inbound Refinery configuration page fields.

Field	Description
Inbound Refinery Instance Folder	Absolute path to the Oracle instance directory of Inbound Refinery. Default is `DomainHome/ucm/` The default Oracle instance directory forInbound Refinery is *`ORACLE_HOME`*`/user_projects/domains/`*`DomainHome`*`/ucm/ibr` 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. Oracle recommends that you make this directory path unique to this Managed Server, or node. For installations that you will probably upgrade, Oracle strongly recommends that you change the location of the Oracle instance directory to a directory outside any Oracle WebLogic Server domain directories or installation directories.
Native File Repository Location	Directory that stores conversion jobs during their processing. After a job converts and Content Server picks it up, it is removed from this directory. You do not need to change this path.
Weblayout Folder	URL for the Inbound Refinery web interface. You do not need to change this path.
Register Start Menu Actions	Whether or not to register Start Menu actions.

Field	Description
Server Socket Port	Number of the port to call 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 also changes the `IntradocServerPort` entry in *`ORACLE_HOME`*`/user_projects/domains/`*`DomainHome`*`/ucm/ibr/config/config.cfg` **Note:** You must set Server Socket Port correctly to useInbound Refinery. **Note:** The default port number for Node Manager and Inbound Refinery is `5555`. If both run on the same server, you must configure a different port number for Node Manager or Inbound Refinery.
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, enter a value for this field. For example: `127.0.0.1|0:0:0:0:0:0:0:1|`*`your.server.IP.address`* This value should be the Content Server instance IP address of the 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 such as 10.*.*.*. You can change this value by setting SocketHostAddressSecurityFilter in DomainHome/ucm/ibr/config/config.cfg and restarting Inbound Refinery. **Note:** To use Inbound Refinery, you must set the Incoming Socket Connection Address Security Filter value correctly.
Web Server HTTP/HTTPS Address	The name of the web server. (HttpServerAddress property).

Field	Description
WebAddress 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	Relative URL for theInbound Refinery instance.
Server Instance Name	Inbound Refinery instance name.
Server Instance Label	Instance name shown for Inbound Refinery.
Service Instance Description	Inbound Refinery Instance description

Configuring WebCenter Content Settings

You must complete the WebCenter Content configuration on the post-installation configuration page in Content Server.

WebCenter Content shows the configuration page when you first sign in to Managed Server at `http://managedServerHost:managedServerPort/cs`

> **Note:**
>
> The domain administrator must be the first user to sign in to the WebCenter Content Managed Server so that they can complete configuration. For more details about administration, see Introduction in *Administering Oracle WebCenter Content*

To complete WebCenter Content configuration:

1. Start the Administration Server. See Starting the Administration Server.
2. Start the WebCenter Content Managed Server. See Starting the Managed Servers.
3. Go to the Content Server post-installation page at `http://managedServerHost:16200/cs/`
4. Enter or edit any configuration values you want to change.

   You can select a full-text search engine in the **FullText Search Option** field. Leave the field blank to set up the system as metadata only.
5. Enter a value in **Incoming Socket Connection Address Security Filter** to enable access from Inbound Refinery. For example:

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

   This field accepts wildcards such as `10.*.*.*` You can change this value later by setting `SocketHostAddressSecurityFilter` in `DomainHome/ucm/cs/config/config.cfg` and restarting WebCenter Content Managed Server.

   For Oracle WSM security, the `SocketHostAddressSecurityFilter` value must be set as follows:

   ```
   SocketHostAddressSecurityFilter=*.*.*.*|0:0:0:0:0:0:0:1
   ```
6. Verify that the **Server Socket Port** setting is `4444`. The Managed Server configuration file stores this value as `IntradocServerPort=4444`
7. Click **Submit**.
8. Restart the WebCenter Content Managed Server. See Starting the Managed Servers

WebCenter Content Configuration Page

You enter or verify values in the WebCenter Content configuration page fields to completeWebCenter Content configuration.

You can use descriptions of these fields while completing steps in Configuring WebCenter Content Settings

Field	Description
Content Server Instance Folder	Absolute path to the Oracle instance directory of WebCenter Content. Default is `DomainHome/ucm/` The default Oracle instance directory forInbound Refinery is *`ORACLE_HOME`*`/user_projects/domains/`*`DomainHome`*`/ucm/cs` 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 WebCenter Content instance. Oracle recommends that you make this directory path unique to this Managed Server, or node. For installations that you will probably upgrade, Oracle strongly recommends that you change the location of the Oracle instance directory to a directory outside any Oracle WebLogic Server domain directories or installation directories.
Native File Repository Location	Path to the vault directory for storing native content checked into WebCenter Content.
Weblayout Folder	Path to the weblayout directory for storing web-viewable renditions of native and alternate files.
Register Start Menu Actions	Whether or not to register Start Menu actions.
Is New Content Server Instance	Whether or not theWebCenter Content instance is new.
Server Socket Port	Number of the port to call top-level services. Default: `5555` To set up a provider from Inbound Refinery back to Content Server, you can leave the default Changing this field value also changes the `IntradocServerPort` entry in *`DOMAIN_HOME`*`/ucm/ibr/config/config.cfg`
Incoming Socket Connection Address Security Filter	Restricts WebCenter Content access to a computer or computers with a specified IP address or addresses. The default value of this field is the local host's IP address, such as `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|`*`your.server.IP.address`* This field accepts wildcards * for zero or many characters, and ? for any one character. (For example, 10.10.3.*) Typically, use the **IP Address Filter** field only (most commoon) or **Hostname Filter** field, not both.
Web Server HTTP/HTTPS Address	Name of the web server. (`HttpServerAddress` property).
WebAddress 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	Relative URL for theInbound Refinery instance.
Server Instance Name	Inbound Refinery instance name.

Field	Description
Server Instance Label	Instance name shown for Inbound Refinery.
Service Instance Description	Inbound Refinery Instance description
Is Auto Number Enabled	Whether or not automatic numbering of WebCenter Contentinstances is enabled.
Auto Number Prefix	Unique prefix for an WebCenter Content instance number, to avoid conflicts among multiple WebCenter Content instances (Auto Number Prefix system property).
FullText Search Option	Search engine for full-text search: **None**: The Oracle Content Server instance uses DATABASE.METADATA as the search engine. **Internal**: If using Oracle Database, the WebCenter Content instance uses OracleTextSearch with the system database. If using Microsoft SQL Server, it will use DATABASE.FULLTEXT. **External**: The Oracle Content Server instance uses OracleTextSearch with an external provider to an Oracle Database (not the system database). If you select this option, you must enter the Data Source name in the External DataSource field.
External DataSource	Name of the Data Source, which you must create in Oracle WebLogic Server and target to the Managed Server, using an OCSSEARCH schema created with Repository Creation Utility (RCU).

Completing the Imaging Configuration

You can complete the initial configuration of Oracle WebCenter Content: Imaging in an Oracle WebLogic Server domain.

This section explains the steps to complete the Imaging configuration.

Completing the Initial Imaging Configuration

Before you complete the configuration of Imaging, your system should have Oracle WebCenter Content installed and configured. Imaging uses WebCenter Content for its repository.

Your Imaging system uses WebCenter Content 14c (14.1.2.0.0) as its document repository. For information about configuring WebCenter Content, see Configuring WebCenter Content Domain.

> **Note:**
>
> In a production system, Oracle WebCenter Content applications 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 association before you complete the configuration of the Imaging Managed Server and before you connect it to the WebCenter Content 14c (14.1.2.0.0) repository. For more information, see 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 as well as the user logging in is given full administrative permissions.

To complete the Imaging configuration, you have to perform all the tasks that apply to your system:

Configuring a WebCenter Content Repository for Imaging

You can configure WebCenter Content 14c (14.1.2.0.0) as the repository for Imaging. You will not be able to import or upload content to the Imaging system unless you have created a repository connection.

Configuring WebCenter Content to Work with Imaging

WebCenter Content 14c (14.1.2.0.0) 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 14c (14.1.2.0.0) 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 before you connect to Oracle WebCenter Content Server from the Imaging web client, as described in 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 14c (14.1.2.0.0) manually to work with Imaging:

1. Start the WebCenter Content Managed Server, as described in Starting the Managed Servers.
2. Access Content Server.
3. Enable the `IpmRepository` component:
    a. From the **Administration** tray or menu, select **Admin Server**, and then select **Component Manager**.
    b. On the Component Manager page, select **Integration**.
    c. Select **IpmRepository**, and click **Update**.

       This option is selected by default if the Oracle WebLogic Server domain is configured with Fusion Middleware Configuration Wizard. If this option is already selected, you can close Component Manager without clicking **Update** or restarting Content Server.
    d. Click **OK**.
    e. Restart Content Server.

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

Configuring a File Store Provider for Content Storage

An administrator can configure a file store provider in Content Server 14c (14.1.2.0.0) 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. See Managing a File Store System in *Administering Oracle WebCenter Content*

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 that is 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 that an administrator defines and configures in Content Server. You cannot use Imaging to create or define a volume.

A Content Server administrator can configure a file store provider. See Managing the File Store Provider in *Administering Oracle WebCenter Content*

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 that you disable the web layout functionality for any file store provider that is configured for use as an Imaging volume.

> **Note:**
>
> 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. See Adding or Editing a Storage Rule in *Administering Oracle WebCenter Content*

Starting the Imaging Managed Server and Accessing the Web Client

You can access the Imaging web client after you start the Administration server and the Imaging and WebCenter Content Managed Servers.

To access the Imaging web client:

1. Start the Imaging Managed Server, as described Starting the Managed Servers.

> **Note:**
>
> If Oracle WebCenter Content: AXF for BPM is deployed to the domain, proceed to Configuring and Verifying AXF for BPM before you perform 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 who connects to the Imaging system is registered as the Imaging administrator.

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 select **Create Content Server Connection** from the list.
4. Enter a name for the connection on the Basic Information page and, optionally, a description, and then click **Next**.
5. Change the selections, if required, on the Connection Settings page:
   - **SSL**: Selected for secure SSL communications.
   - **Server Port**: The IDC port of the WebCenter Content instance. By default, 4444 for Imaging.
   - **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, 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 other users 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**.

Connecting to a Workflow Server

A connection to a workflow server (Oracle SOA Suite) is required before you import the definition files. This connection is 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 - 14.1.2.0.0**. When Oracle BPM Suite is installed, it automatically selects **Oracle SOA Suite - 14.1.2.0.0** 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. See About the Oracle SOA Suite and Oracle Business Process Management Installation in *Installing and Configuring Oracle SOA Suite and Business Process Management*.

This section describes the procedure 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*.

Configuring a Connection to a Workflow Server

If you have installed the Oracle SOA Suite for use with Imaging, 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 select **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 other users 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**.

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`.

Configuring the GDFontPath MBean for a UNIX System

For conversions to work correctly on a UNIX operating system, the operating system 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 by using the 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. For example: `http://myHost.example.com:7001/em`

   To log in, provide 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 select **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.

Setting DISPLAY for the Imaging Viewer in a UNIX Exalogic Environment with Solaris 12*c*

In an Exalogic environment with Solaris 12*c*, you need to set the DISPLAY environment variable for the Imaging Viewer to work correctly in the basic mode.

To set DISPLAY for the Imaging Viewer in a UNIX Exalogic Environment with Solaris 12*c*:

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 specify the port, in this format:

   ```
   servername:port
   ```

3. Restart Imaging.

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 Importing Definition Files into Imaging.

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.

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 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. See Configuring System Properties in *Administering Oracle WebCenter Content*.

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 the initial user's 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. Otherwise, you will not get 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 the Imaging system security.

1. Manually create or migrate users and groups to the new external security provider, using utilities as needed. See Reassociating the Identity Store with an External LDAP Authentication Provider.
2. Run the `refreshIPMSecurity() WLST MBean` command. See refreshIPMSecurity in *WebCenter WLST 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.

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 the documents are stored.

If the server is considered secure, no additional security is necessary. If additional security is required, you can encrypt cached documents as described in 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 Remote Console, click **Deployments** under Domain Structure.
   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 you proceed.
2. Enable viewer caching by setting the **ViewerCachePath** MBean to the location where the documents must be cached, as described in Configuring the GDFontPath MBean for a UNIX System. For example, to enable caching on an Imaging system that runs on a single

computer, you can use the relative path `imaging/ViewerCache`. If no path is set, then caching of documents is disabled.

> **Note:**
>
> The **ViewerCachePath** MBean must be set to a location that is available to all the servers in the cluster. If the directory path is not available to all the servers, 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. If you set **ViewerCacheDays** equal to `0` (the default), you cannot purge the documents from cache.
4. Set the **ViewerCacheEnablePrecache** MBean to `true` to cache documents when they are ingested into Imaging (pre-cache) or set the value to `false` to cache documents when they are first called by the viewer.

Changing the Viewer Cache Path

You can move the viewer cache to a new location if the Imaging server is shut down and the new location uses the same file hierarchy as the old location.

To change the viewer cache path:

1. Shut down the Imaging server.
2. Move the cached files to the new location. Ensure that you preserve the file hierarchy.
3. Set the new path in the **ViewerCachePath** MBean.
4. Start the Imaging server.

Encrypting Cached Documents

For additional security, you an configure Imaging to encrypt the cached documents. Encryption makes additional processing necessary to decrypt a document for viewing, and reduces the rendering speed. Even if you configure Imaging to encrypt the cached documents, there is a brief period of time during caching when the documents that are generated 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 there is no map named oracle.imaging, click **Create Map**, specify `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, as described in Configuring the GDFontPath MBean for a UNIX System.

> **Note:**
>
> The password credential must exist on the domain before you set the **ViewerCacheEnableEncryption** MBean.

Disabling Encryption of Cached Documents

You can disable the encryption of cached documents by setting the value of the **ViewerCacheEnableEncryption** MBean to `false`.

Subsequent calls to the viewer causes unencrypted documents to be cached. You can decrypt and view any encrypted documents that are already in the cache if the password credential remains unaltered in the domain.

If you removed or alter the password credential, you must manually purge the encrypted documents that are still cached.

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.

Installing and Configuring AXF 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. Then when the domain is created or extended, you can select AXF for BPM to use it with Imaging.

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 that are 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. These business components help administrators to configure and develop integration solutions for WebCenter Content business applications. See Configuring and Verifying AXF for BPM.

- AXF for BPEL

  You can configure AXF for BPEL to run on the Imaging Managed Server. 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. See 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 Configuring the BPEL Imaging Solution in *Administering the Application Adapters for Oracle WebCenter*.

Configuring and Verifying AXF for BPM

Before you configure AXF for BPM with Imaging, you need to install and configure 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, you need to extend the domain 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. You can also 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. See Configuring AXF for BPM.

To verify that you have installed and configured the AXF for BPM infrastructure properly, AXF for BPM includes the *HelloBPM* solution, which uses an Oracle BPM process to verify the BPM integration. See Verifying the AXF for BPM Installation.

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. See Oracle Coherence Communications for Imaging Clusters, Multiple Domains, or Multiple Machines. In a single domain, you can set up communications with Oracle Coherence to avoid interference from multicast traffic. See Oracle Coherence Communications for a Single Server or Domain.

To configure AXF for BPM:

1. Set up the Imaging server through the WebLogic Remote Console:
   a. The Administration Server should be running. If not, start the Administration Server for your Oracle WebLogic Server domain. See Starting the Administration Server.
   b. Log in to the Remote 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, click **Lock & Edit** in the Change Center on the left before you make changes.
   f. Click the **HTTP** tab and 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`.
   g. Save the changes.

      If the server is in production mode, activate changes after you save them, unless you have enabled configuration editing.
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 Remote Console.
   b. Under **Domain Structure** on the left, expand **Services**, and click **Data Sources**.
   c. Select **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 Remote 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, select **Generic Data Source** from the **New** menu.

   d. In the **Name** field, specify `SOALocalTxDataSource`.

   e. In the **JNDI** Name field, specify `jdbc/SOALocalTxDataSource`.

   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 the 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 by 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, select **Security**, and then **Credentials**.

d. Create a new map, specify the map name as `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.
- Click **OK**.

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, Using Coherence Clusters in *Developing Applications with Oracle Coherence*

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 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.

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. This section describes the procedure to deploy and use this solution.

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, which will insert the data necessary to run the HelloBPM solution:
      - `SOAMachineName:Port`
      - `IPMMachineName:Port`
      - `CSFKEY`
2. If the Oracle SOA Suite Managed Server is on a separate host machine from Imaging, you will need to manually deploy the Hello BPM process. 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:
   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`

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. See Completing the Initial Imaging Configuration.

b. In the navigation tree on the left, expand **Manage Connections**.

c. Select **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. Select **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 that was specified in Step 5 of Configuring and Verifying AXF for BPM, 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 About Imaging in *Administering Oracle WebCenter Content: Imaging*.

   a. In the navigation tree on the left, expand **Tools**.

   b. Select **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 **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, select the **Administrators** group for the **Applications**, **Document Security**, **Inputs Security**, and **Searches Security** fields.

h. For the **Workflow** field, select **Workflow Connection**.

i. Click **Submit**.

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.

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 **Execute Request**.
5. Click **Execute Response**.

The Solution Administration page opens. Table 4-1 shows the example parameters for this page.

Table 4-1 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.

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. 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.

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. See Clustering for AXF in 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.
- `HelloBpel`, a solution that includes a BPEL process to verify the BPEL integration.

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.

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, 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 by 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 sign 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.

Configuring Capture

The Capture System Administrator requires system administration privileges to configure and monitor an Oracle WebCenter Enterprise Capture system environment. The configuration consists of tasks such as starting the Capture Managed Server, assigning roles to Capture users in Fusion Middleware Control, and modifying system-level settings through MBeans.

This appendix explains the configuration tasks in detail.

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.

Through Fusion Middleware Control, you can also configure system settings and loggers for Capture.

Completing the Initial Configuration of Oracle WebCenter Enterprise Capture

The Capture System Administrator performs the initial configuration of Capture in a WebLogic Server domain. In addition to starting the Capture Managed Server, the configuration steps also include assigning roles to users and modifying system-level settings.

Starting the Capture Managed Server

The first step to complete Capture configuration is to start the Capture Managed Servers.

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.

To assign roles to Capture users, see Assigning Capture Roles in Oracle Enterprise Manager in *Administering Oracle WebCenter Enterprise Capture*.

Modifying System-Level Settings

You can modify system-level configuration settings for Capture, including system properties and SMTP settings for e-mail, 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.

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.
2. Sign in to the Oracle WebLogic Server Administration Server.
3. Navigate to the Oracle WebCenter Content home directory at *`MW_HOME/WCC_ORACLE_HOME`*
4. Run WLST.

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

5. Sign 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:9225
   ```

```
Connecting to t3://host_name:9225 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()
```

5

Next Steps After Configuring the Domain

After you configure a product domain, there are additional tasks that you may want to perform.

Performing Basic Administrative Tasks

After you configure your new domain, there are administration tasks that Oracle recommends you perform on the domain.

The following table lists common administration tasks to perform on your new domain.

Table 5-1 Basic Administration Tasks for a New Domain

Task	Description	More Information
Getting familiar with Fusion Middleware administration tools	Get familiar with various tools that you can use to manage your environment. **Note:** The WebLogic Server Administration Console has been removed. For comparable functionality, you will use the WebLogic Remote Console.	See Overview of Oracle Fusion Middleware Administration Tools in *Administering Oracle Fusion Middleware*.
Starting and stopping products and servers	Learn how to start and stop Oracle Fusion Middleware, including the Administration Server, Managed Servers, and components.	See Starting and Stopping Oracle Fusion Middleware in *Administering Oracle Fusion Middleware*. For secured production mode procedures for starting and stopping servers, see Using Secured Production Mode in *Administering Security for Oracle WebLogic Server*

Table 5-1 (Cont.) Basic Administration Tasks for a New Domain

Task	Description	More Information
Configuring Secure Sockets Layer (SSL)	Learn how to set up secure communications between Oracle Fusion Middleware components using SSL.	See Configuring SSL in Oracle Fusion Middleware in *Administering Oracle Fusion Middleware*. For secured production mode procedures for SSL, see Configuring SSL in *Administering Security for Oracle WebLogic Server*.
Monitoring Oracle Fusion Middleware	Learn how to keep track of the status of Oracle Fusion Middleware components.	See Monitoring Oracle Fusion Middleware in *Administering Oracle Fusion Middleware*.
Understanding Backup and Recovery Procedures	Learn recommended backup and recovery procedures for Oracle Fusion Middleware.	See Introducing Backup and Recovery in *Administering Oracle Fusion Middleware*.

Performing Additional Domain Configuration Tasks

Review additional configuration tasks you will likely want to perform on a new domain.

Table 5-2 Additional Domain Configuration Tasks

Task	Description	More Information
Deploying Applications	Learn how to deploy your applications to Oracle Fusion Middleware.	See Deploying Applications in *Administering Oracle Fusion Middleware*.
Adding a Web Tier front-end to your domain	Oracle Web Tier hosts Web pages (static and dynamic), provides security and high performance along with built-in clustering, load balancing, and failover features. In particular, the Web Tier contains Oracle HTTP Server.	To install and configure Oracle HTTP Server in the WebLogic Server domain, see Configuring Oracle HTTP Server in a WebLogic Server Domain in *Installing and Configuring Oracle HTTP Server*. See also Installing Multiple Products in the Same Domain for important information.
Tuning and configuring Coherence for your topology	The standard installation topology includes a Coherence cluster that contains storage-enabled Managed Coherence Servers. This configuration is a good starting point for using Coherence, but depending upon your specific requirements, consider tuning and reconfiguring Coherence to improve performance in a production environment.	For more information about Coherence clusters, see Configuring and Managing Coherence Clusters in *Administering Clusters for Oracle WebLogic Server*. For information on tuning Coherence, see Performance Tuning in *Administering Oracle Coherence*. For information on storing HTTP session data in Coherence, see Using Coherence*Web with WebLogic Server in *Administering HTTP Session Management with Oracle Coherence*Web*. For more about creating and deploying Coherence applications, see Getting Started in *Developing Oracle Coherence Applications for Oracle WebLogic Server*.

Preparing Your Environment for High Availability

Scaling out for high availability requires additional steps.

Table 5-3 provides a list of tasks to perform if you want to scale out your standard installation environment for high availability.

> **Note:**
>
> BAM domains that were created using WLST, and will be used in a high availability configuration, require additional provisioning scripts after the installation. The default / internal Data Objects are missing in BAM Composer when the domain is created using WLST and the scripts provide the pre-seeded data that is required for high availability BAM domains. For more information, My Oracle Support document ID 2190789.1.
>
> .

Table 5-3 Tasks Required to Prepare Your Environment for High Availability

Task	Description	More Information
Scaling out to multiple host computers	To enable high availability, it is important to provide failover capabilities to another host computer. That way, if one computer goes down, your environment can continue to serve the consumers of your deployed applications.	See Scaling Out a Topology (Machine Scale Out) in *High Availability Guide*.
Configuring high availability for your Web Tier components.	If you have added a Web tier front-end, then you must configure the Web Tier for high availability, as well as the WebLogic Server software.	See Configuring High Availability for Web Tier Components in *HTTP Server Administration Guide*.
Setting up a front-end load balancer	You can use a load balancer to distribute requests across servers more evenly.	See Server Load Balancing in a High Availability Environment in *High Availability Guide*.
Configuring Node Manager	Node Manager enables you to start, shut down, and restart the Administration Server and Managed Server instances from a remote location. This document assumes you have configured a per-domain Node Manager. Review the Node Manager documentation, for information on advanced Node Manager configuration options and features.	See Advanced Node Manager Configuration in *Administering Node Manager for Oracle WebLogic Server*.

Configuring WebCenter Content User Interface on Additional Nodes

If you install WebCenter Content User Interface on one node, its configuration is complete. However, if you scale out WebCenter Content User Interface to a second node (in a high availability or enterprise deployment topology, for example), you must complete additional configuration steps.

To run WebCenter Content User Interface on additional nodes, you must:

- Enable WebCenter Content User Interface components.
- Set the server socket port to 4444.

To enable WebCenter Content User Interface components:

1. Sign in to WebCenter Content 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** then click **OK** to confirm that you want to enable the components.
5. Restart WebCenter Content. See Starting and Stopping Managed Servers in *Administering Oracle Fusion Middleware*.

Continue to the topic Setting the WebCenter Content User Interface Server Socket Port.

> **Note:**
>
> You may find following exception setting up file watcher for LCM Configuration File: `java.io.IOException: User limit of inotify instances reached or too many open files`
>
> Run the following commands to resolve this exception:
>
> ```
> echo 256 > /proc/sys/fs/inotify/max_user_instances
> ```
>
> ```
> ulimit -n 10000
> ```

Setting the WebCenter Content User Interface Server Socket Port

If you are scaling out WebCenter Content User Interface you must change the server socket port.

To change the server socket port:

1. Open `WCC_DOMAIN/ucm/cs/config/config.cfg`
2. Set `IntradocServerPort` to `4444`.

   ```
   IntradocServerPort=4444
   ```

Configuring WebCenter Content User Interface Settings

You set WebCenter Content User Interface connection and configuration settings with WLST or Fusion Middleware Control.

Setting Connection Attributes with WLST

You can use `displayRIDCConnection` and `updateRIDCConnection` WLST commands to read and update connection properties.

For example, to update the RIDC connection to the WebCenter Content User Interface Managed Server:

1. Run WLST from *`ORACLE_HOME`*`/oracle_common/common/bin/wlst.sh`.
2. Enter `wls:/offline> connect()` and enter your username and password at the prompt.
3. Enter the Managed Server URL, for example, `t3://localhost:9225`

   9225 is the default administration port for WebCenter Content in 14c (14.1.2.0.0) WebLogic Server secured setup. If you have configured a custom administration port for WebCenter Content user interface, then use the custom administration port.
4. Update the RIDC connection to the WebCenter Content User Interface Managed Server. For example:

   ```
   wls:/mydomain/serverConfig>updateRIDCConnection('Oracle WebCenter
   Content - Web UI','WccAdfServerConnection',connUrl='idc://
   contentserver_host:intradoc_port',credUsername='ucm_admin_user')
   ```
5. Restart the Managed Server.

Setting Connection Attributes with Fusion Middleware Control

Instead of using WLST, you can set connection attributes for WebCenter Content User Interface Managed Server with the Fusion Middleware Control System MBean Browser.

To set connection attributes through Fusion Middleware Control:

1. Sign 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 WebCenter Content User Interface domain folder, then the cluster name, and then click Managed Server name.
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, navigate to the **WccAdfServerConnection** MBean. To do this, expand **Application Defined MBeans** —> **oracle.adf.share.connections** —> **Server: WCCADF_server1** —> **Application: Oracle WebCenter Content – Web UI**. Expand the Mbean **ADFConnections** then the folder **WccConnection**.
   - Instead of opening up the folder, you can enter the connection name **WccAdfServerConnection** in the MBean filtered search.
5. Click the MBean **WccAdfServerConnection**.
6. In the **Attributes** tab, select **PropConnectionURL**. Enter a URL to set up the RIDC connection. Click **Apply** (top right)

   If you leave the **PropConnectionSocketTimeout** attribute blank, the default (60 seconds) becomes the RIDC Connection Socket Timeout value. This value can create problems if you download large files that are being converted to TIFF or PDF documents with annotations burned in. You can set the attribute to a larger value if you have large files.

7. Go back to the **ADFConnections** page (**Application Defined MBeansoracle.adf.share.connectionsServer: WCCADF_server1Application: Oracle WebCenter Content – Web UIADFConnections**).
8. On the Operations tab, click save. Then click **Invoke**.
9. Restart the WebCenter Content User Interface Managed Server.

Setting Configuration Attributes with WLST

You can use WLST commands `displayWccAdfConfig` and `updateWccAdfConfig` to read and update WebCenter Content User Interface configuration parameters.

For example, to use `updateWccAdfConfig` to update the application's URL:

1. Run WLST from *`ORACLE_HOME`*`/oracle_common/common/bin/wlst.sh`.
2. Enter `wls:/offline> connect()` and enter your username and password at the prompt.
3. Enter the Managed Server URL, for example, `t3://localhost:9225`

   9225 is the default administration port for WebCenter Content in 14c (14.1.2.0.0) WebLogic Server secured setup. If you have configured a custom administration port for WebCenter Content user interface, then use the custom administration port.
4. Update the WebCenter Content User Interface Managed Server. For example:

   ```
   wls:/mydomain/serverConfig>updateWccAdfConfig('Oracle WebCenter
   Content - Web UI',applicationUrl='idc://
   contentserver_host:intradoc_port')
   ```
5. Restart the WebCenter Content User Interface Managed Server.

Setting Configuration Attributes with Fusion Middleware Control

Instead of using WLST, you can set configuration (**WccAdfConfiguration**) attributes for WebCenter Content User Interface Managed Server with the Fusion Middleware Control System MBean Browser.

For example, to set the WebCenter Content User Interface application URL:

1. Sign 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 WebCenter Content User Interface domain folder, then the cluster name, and then click Managed Server name.
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, navigate to the **WccAdfConfiguration** MBean. To do this, expand **Application Defined MBeans** —> **oracle.adf.share.config** —> **Server: WCCADF_server1** —> **Application: Oracle WebCenter Content – Web UI**. Expand the folder **ADFConfig**, the Mbean **ADFConfig** , then the folder **ADFConfig**.
   - Instead of opening up a series of folders to reach the MBean, you can enter the connection name **WccAdfConfiguration** in the MBean filtered search.
5. Click the MBean **WccAdfConfiguration**.
6. In the **Attributes** tab, select **ApplicationUrl**. In the **Value** field, enter the base application URL. For example: `https://wcc.`*`example`*`.com:9225`. Click **Apply** (top right)

7. Go back to the **ADFConfig** MBean page (**Application Defined MBeans —> oracle.adf.share.config —> Server: WCCADF_server1 —> Application: Oracle WebCenter Content – Web UI —> ADFConfig**).
8. On the Operations tab, click save then **Invoke**.
9. Restart the WebCenter Content User Interface Managed Server.

6

Uninstalling or Reinstalling Oracle WebCenter Content

Follow the instructions in this section to uninstall or reinstall Oracle WebCenter Content.

Oracle recommends that you always use the instructions in this section to remove the software. If you try to remove the software manually, you may encounter problems when you try to reinstall the software again at a later time. Following the procedures in this section ensures that the software is properly removed.

About Product Uninstallation

The Oracle Fusion Middleware uninstaller removes the software from the Oracle home directory.

The following table summarizes the tasks to uninstall Fusion Middleware products.

Table 6-1 Roadmap for Product Uninstallation

Task	Description	Documentation
Stop Oracle Fusion Middleware	All servers and processes in your domain should be stopped before running the uninstaller.	See Stopping Oracle Fusion Middleware.
Remove your database schemas	Run Repository Creation Utility to remove your database schemas.	See Removing Your Database Schemas.
Remove the software	Run the product uninstaller to remove Oracle Fusion Middleware Infrastructure. Note that if your Oracle home contains multiple products, you must run the uninstaller multiple times, once for each product.	See Uninstalling the Software.
Remove the Oracle home directory	The uninstaller does not remove all files and folders from the Oracle home directory. After the uninstaller is finished, you must manually remove the Oracle home to complete your product removal.	See Removing the Oracle Home Directory Manually.
Remove your domain and application data	The uninstaller does not remove data contained in your Domain home or Application home directories, even if they are located inside the Oracle home. You must remove these directories manually.	See Removing the Domain and Application Data.

Stopping Oracle Fusion Middleware

Before running the Uninstall Wizard, Oracle recommends that you stop all servers and processes associated with the Oracle home you are going to remove.

See Stopping an Oracle Fusion Middleware Environment in *Administering Oracle Fusion Middleware*.

Removing Your Database Schemas

Before you remove the Oracle home, Oracle recommends that you run the Repository Creation Utility (RCU) to remove database schemas associated with this domain.

Each domain has its own set of schemas, uniquely identified by a custom prefix. For more information about custom prefixes, see About Custom Prefixes in *Creating Schemas with the Repository Creation Utility*. This set of schemas cannot be shared with any other domain. For more information about creating schemas with the RCU, see Planning Your Schema Creation in *Creating Schemas with the Repository Creation Utility*.

If there are multiple sets of schemas on your database, be sure to identify the schema prefix associated with the domain that you are removing.

For schema removal steps, see Dropping Schemas in *Creating Schemas with the Repository Creation Utility*.

Uninstalling the Software

Follow the instructions in this section to start the Uninstall Wizard and remove the software.

If you want to uninstall the product in a silent (command-line) mode, see Running the Oracle Universal Installer for Silent Uninstallation in *Installing Software with the Oracle Universal Installer*.

Starting the Uninstall Wizard

To start the Uninstall Wizard:

1. Change to the following directory:

   (UNIX) *ORACLE_HOME*`/oui/bin`

   (Windows) *ORACLE_HOME*`\oui\bin`
2. Enter the following command:

   (UNIX) `./deinstall.sh`

   (Windows) `deinstall.cmd`

Selecting the Product to Uninstall

Because multiple products exist in the Oracle home, ensure that you are uninstalling the correct product.

After you run the Uninstall Wizard, the Distribution to Uninstall screen opens. From the dropdown menu, select **fmw_14.1.2.0.0_wccontent.jar** and click **Uninstall**. The uninstallation program shows the screens listed in Navigating the Uninstall Wizard Screens.

> **Note:**
>
> You can uninstall Oracle Fusion Middleware Infrastructure after you uninstall Oracle WebCenter Content software by running the Uninstall Wizard again. Before doing so, make sure that there are no other products using the Infrastructure; those products will no longer function once the Infrastructure is removed. You will not encounter the Distribution to Uninstall screen if no other software depends on Oracle Fusion Middleware Infrastructure. See Uninstalling Oracle Fusion Middleware Infrastructure in *Installing and Configuring the Oracle Fusion Middleware Infrastructure*.

Navigating the Uninstall Wizard Screens

The Uninstall Wizard shows a series of screens to confirm the removal of the software.

If you need help on screen listed in Table 6-2, click **Help** on the screen.

Table 6-2 Uninstall Wizard Screens and Descriptions

Screen	Description
Welcome	Introduces you to the product Uninstall Wizard.
Uninstall Summary	Shows the Oracle home directory and its contents that are uninstalled. Verify that this is the correct directory. If you want to save these options to a response file, click **Save Response File** and enter the response file location and name. You can use the response file later to uninstall the product in silent (command-line) mode. See Running the Oracle Universal Installer for Silent Uninstall in *Installing Software with the Oracle Universal Installer*. Click **Deinstall**, to begin removing the software.
Uninstall Progress	Shows the uninstallation progress.
Uninstall Complete	Appears when the uninstallation is complete. Review the information on this screen, then click **Finish** to close the Uninstall Wizard.

Removing the Oracle Home Directory Manually

After you uninstall the software, you must manually remove your Oracle home directory and any existing subdirectories that the Uninstall Wizard did not remove.

For example, if your Oracle home directory is `/home/Oracle/product/ORACLE_HOME` on Linux operating systems, enter the following commands:

```
cd /home/Oracle/product
rm -rf ORACLE_HOME
```

On Windows operating systems, if your Oracle home directory is `C:\Oracle\Product\ORACLE_HOME`, use a file manager window and navigate to the `C:\Oracle\Product` directory. Right-click on the *ORACLE_HOME* folder and select **Delete**.

Removing the Program Shortcuts on Windows Operating Systems

On Windows operating systems, you must also manually remove the program shortcuts; the Deinstallation Wizard does not remove them for you.

To remove the program shortcuts on Windows:

1. Change to the following directory: `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Oracle\ORACLE_HOME\Product`
2. If you only have one product installed in your Oracle home, delete the *ORACLE_HOME* directory. If you have multiple products installed in your Oracle home, delete all products before you delete the *ORACLE_HOME* directory.

Removing the Domain and Application Data

After you uninstall the software, you must remove the domain and application data.

To remove the domain and application data:

1. Manually remove your Domain home directory. For example:

   On a UNIX operating system, if your Domain home directory is `/home/Oracle/config/domains/wcc_domain`, enter the following command:

   ```
   cd /home/Oracle/config/domains
   rm -rf wcc_domain
   ```

   On a Windows operating system, if your Domain home directory is `C:\Oracle\Config\domains\wcc_domain`, use a file manager window and navigate to the `C:\Oracle\Config\domains` directory. Right-click on the `wcc_domain` folder and select **Delete**.

2. Manually remove your Application home directory. For example:

   On a UNIX operating system, if your Application home directory is `/home/Oracle/config/applications/wcc_domain`, enter the following commands:

   ```
   cd /home/Oracle/config/applications
   rm -rf wcc_domain
   ```

   On a Windows operating system, if your Application home directory is `C:\Oracle\Config\applications\wcc_domain`, use a file manager window and navigate to the `C:\Oracle\Config\applications` directory. Right-click on the `wcc_domain` folder and select **Delete**.

3. Back up the `domain_registry.xml` file in your Oracle home, then edit the file and remove the line associated with the domain that you are removing. For example, to remove the `wcc_domain`, find the following line and remove it:

   ```
   <domain location="/home/Oracle/config/domains/wcc_domain"/>
   ```

   Save and exit the file when you are finished.

Reinstalling the Software

You can reinstall your software into the same Oracle home as a previous installation only if you uninstalled the software by following the instructions in this section, including manually removing the Oracle home directory.

When you reinstall, you can then specify the same Oracle home as your previous installation.

If ODI is installed again in the same location where it was previously deleted, delete the entire Oracle Home where it was previously installed.

Consider the following cases where the Oracle home is not empty:

- Installing in an existing Oracle home that contains the same feature sets.

  The installer warns you that the Oracle home that you specified during installation already contains the same software you are trying to install.

- Installing in an existing, non-empty Oracle home.

  For example, suppose you chose to create your Domain home or Application home somewhere inside your existing Oracle home. This data is not removed when you uninstall a product, so if you try to reinstall into the same Oracle home, the installer does not allow it. Your options are:

  – Uninstall your software from the Oracle home (as this section describes) and then remove the Oracle home directory. After you uninstall the software and remove the Oracle home directory, you can reinstall and reuse the same Oracle home location. Any domain or application data that was in the Oracle home must be re-created.

  – Select a different Oracle home directory.

A

Configuring Content Server

You can configure Content Server for Desktop, Records Management, and Oracle iPlanet Web Server.

Configuring Records Management in Content Server

If you are licensed to configure the Records Management in a WebCenter Content Managed Server, you can configure either a standalone Records Management, a universal (or fully functional) Records Management, or the Oracle URM Adapter in Content Server after you configure the WebCenter Content Records Managed Server.

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

If you don't want to use Records Management in the Content Server, you can remove the configuration user interface by disabling the RMFeatureConfig component. Before you disable the Records Management and restart the Content Server, you need to delete the Report template files that Records Management installs. You cannot delete them after Records Management is disabled.
To configure Records Management in the Content Server:

1. From the **Administration** 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, and click **Submit**.
    - **None**: No Records Management functionality is configured.
    - **Standalone**: Enables basic Records Management functionality on Content Server.
    - **Universal**: Enables full Records Management functionality on Content Server. This includes Physical and External sources.
    - **Adapter**: Enables Universal Content Management Adapter functionality on Content Server.
3. Restart the WebCenter Content Managed Server. See Starting and Stopping Managed Servers.

    After you restart the WebCenter Content, Records Management Setup checklist appears.
4. If you selected **Adapter**, click **Register Source** on the Enabled Features page then enter values for the fields on the Register Source page:

Option	Description
Provider Name	Outgoing provider used to connect to the Records Managed Server. You can choose from the list of current outgoing providers, or you can click **Add** and create one. 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	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	Prefix to use for creating database tables. The default value is the source name.
Source Display Name	Caption to use for showing the source name. Default value is the source name.

5. Click **Register**.

   Before the source is 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 if any items in the adapter are missing in the Records server. Before you can register the source, you must resolve any differences on the Import Retention Schedule page.

   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.

6. After the source is successfully registered, click **OK** on the confirmation page.

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

7. Configure the adapter in the Configuration Wizard:

Table A-1 Adapter Options

Option	Description
Configure Custom Fields	Page where you enter 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 Serve, or you can rename the field. When the content is uploaded to the Records server as external content items, these fields map to their external field names. You can configure the following custom fields: • Add or edit an external custom field • Configure the disposition actions or scheduled events • View the external source information

Table A-1 (Cont.) Adapter Options

Option	Description
Configure Scheduled Times	Page where you enter when the scheduled tasks run. You can specify the interval at which the tasks are run (in hours, days, or weeks) and the time of day.

8. From the **Records** menu, select **Configure** 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..

> **Note:**
>
> If you have changed any features or dispositions, restart the WebCenter Content.

About Configuring Oracle iPlanet Web Server as a Web Tier and Configuring Shared Folders

You can configure the Oracle iPlanet Web Server as a web tier for WebCenter Content. If you are using a cluster of WebCenter Content Managed Servers, you need to configure a shared file system for the WebCenter Content cluster.

Configuring the Content Server for Desktop

You need to make sure the CoreWebdav system component is enabled, before the client can use the WebCenter Content Desktop with the Content Server.

Additionally, you must enable the following components:

- DesktopIntegrationSuite
- DesktopTag
- FolderStructureArchive
- FrameworkFolders

> **Note:**
>
> Windows 10 and MS Office 2016 is supported in the DesktopIntegrationSuite (DIS).

You can also enable the EmailMetadata, which maps the e-mail message fields to the e-mail metadata fields.

> **Note:**
>
> When you enable the FrameworkFolders component (Folders feature), verify that the Folders_g component (Contribution Folders feature) is disabled; CoreWebdav will not work correctly with both enabled.

To configure the Content Server for Desktop:

1. Sign in to WebCenter Content as an administrator.
2. In the Content Server Administration menu, select **Admin Server** then select **Component Manager**. .
3. On the Component Manager page, select **Folders** to display the Folders category of components.
4. Select the following components:
   - FrameworkFolders
   - DesktopIntegrationSuite
   - DesktopTag
   - (Optional) EmailMetadata
5. Click **Update** then click **OK** to confirm your selections.
6. In the Component Manager page, click **advanced component manager**.
7. In the Disabled Components box on the Advanced Component Manager page, select FolderStructureArchive, and click **Enable**.
8. If Folders_g is in the Enabled Components box, select this component and click the **Disable**.
9. Make sure that the CoreWebdav component is enabled:
   - Under Category Filters on the Advanced Component Manager page, select **Show System Components**.
   - If CoreWebdav is not in the Enabled Components box, select **CoreWebdav** in the Disabled Components box and click **Enable**.
10. Restart the Content Server, as Starting and Stopping Managed Servers describes.

See the remaining topics in this section for more on configuration tasks.

About Installing and Configuring the Desktop on a Client Workstation

WebCenter Content for desktop has a set of embedded applications that help users integrate desktop experiences with Content Server, Oracle Content Database, or other WebDAV-based content repositories.

These applications provide convenient access to content repositories directly from Microsoft Windows Explorer, Microsoft Office applications, and supported e-mail clients (Microsoft Outlook and Lotus Notes).To install Desktop on a client workstation, see Setting Up the Desktop Client Software on Your Computer.

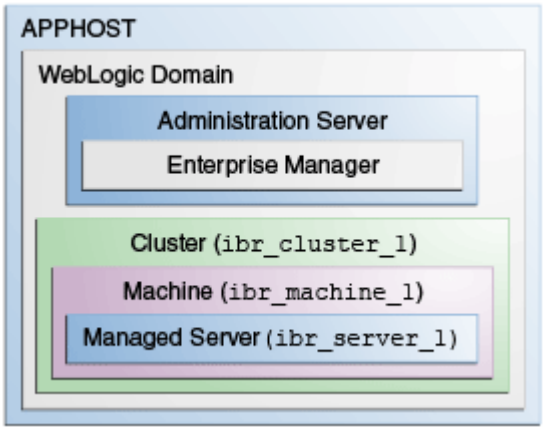
B

Inbound Refinery Standalone Topology

The most common installation topology for Inbound Refinery is a standalone instance of one Inbound Refinery Managed Server on its own host. There are no other components in the domain.

The following figure shows a typical installation topology for Inbound Refinery. This topology consists of an Administration Server and one Oracle WebLogic Server domain on a single host. The cluster has one Inbound Refinery Managed Server.

> **Note:**
>
> Inbound Refinery in a standalone topology does not need a database connection or database installation. However, you must still run RCU and select certain options.



Roadmap for Installing and Configuring the Inbound Refinery Standalone Topology

This roadmap has the steps required to install and configure a standalone instance of Inbound Refinery .

Complete each roadmap task in the order that the following table describes.

Table B-1 Standard Installation Roadmap

Task	Description	More Information
Verify your system environment	Before beginning the installation, verify that the minimum system and network requirements are met.	See Roadmap for Verifying Your System Environment.

Table B-1 (Cont.) Standard Installation Roadmap

Task	Description	More Information
Check for any mandatory patches that will be required before or after the installation	Review the Oracle Fusion Middleware Infrastructure release notes to see if there are any mandatory patches required for Inbound Refinery.	See Install and Configure in *Release Notes for Oracle Fusion Middleware Infrastructure*.
Obtain the appropriate distributions	Install Oracle Fusion Middleware Infrastructure to create the Oracle Home for Oracle WebCenter Content	See About Product Distributions.
Determine your installation directories	Verify that the installer can access or create the installer directories that it must access or create. Also, verify that the directories exist on systems that meet the minimum requirements.	See What are the Key Oracle Fusion Middleware Directories? in *Understanding Oracle Fusion Middleware*.
Install prerequisite software	Install Oracle Fusion Middleware Infrastructure to create the Oracle home directory for Inbound Refinery.	For Oracle Fusion Middleware Infrastructure , see Installing the Infrastructure Software. You only need to perform the installation for Infrastructure. You do not need to configure a domain for Infrastructure.
Install the software	Run the Oracle Universal Installer to install Inbound Refinery. Installing the software transfers the software to your system and creates the Oracle home directory.	See Installing the Oracle WebCenter Content Software. Return to this roadmap for instructions on RCU.
Create the schemas	Run the Repository Creation Utility to create the schemas required for configuration. **Note**: Configuration Requires requires that you run RCU. However, the Inbound Refinery standalone installation does not require a database connection.	1. Navigate to the *ORACLE_HOME*`/oracle_common/bin` directory on your system. 2. Run RCU. On UNIX systems, enter `./rcu`. On Microsoft Windows, run `rcu.bat` 3. Select **System Load and Product Load**. 4. Click **Next**. 5. Enter database connection details. 6. Select **Oracle Platform Security Services**, which selects other required schemas such as **Audit Services**.
Create a WebLogic domain	Use the Configuration Wizard to create and configure the WebLogic domain. Note that the domain will have a cluster that has only *one* Managed Server.	See Configuring the Domain if you are creating the topology for Oracle WebCenter Content.

C

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 the 32-bit binaries and have compatible libraries installed.

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.

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
    ```

    Restart inbound Refinery.
  - 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.

D

Additional Configuration Steps

See the following topics for additional Oracle WebCenter Content configuration steps.

Converting Vector Graphics and Spreadsheet Text in UNIX

Dynamic Converter requires access to a running X-Server in UNIX in order to convert vector graphics and to properly measure text that spans multiple columns in spreadsheets.

Access to a running X-server is required only if the OIT internal rendering engine is not used because of either of the following reasons:

- The **Use X-Windows for Rasterization** option is checked on the Dynamic Converter configuration page.
- The OIT internal rendering engine isn't supported on the platform being used.

The internal OIT rendering engine is supported in Linux, Solaris Sparc, AIX, and HP-UX RISC.

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.

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.

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. Sign 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**.

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.

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 11g 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.

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.

LDAP Authentication Provider	Authentication 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, sign in to the management console as a user from Oracle Internet Directory, to be the Oracle IRM domain administrator.

   Do not sign 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 signed in to 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.
   b. Sign in to the Oracle WebLogic Server Administration Console as the domain administrator user, at this URL: `http://adminServerHost:adminServerPort/console`

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.

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. 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.

   - 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.

I. Click **Save**.

6. Restart the Administration 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, sign 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:

11. For an Oracle IRM Managed Server, if a user has already signed in to 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: 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.

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.

Configuring OracleTextSearch for Content Server

If you have a license to use OracleTextSearch (with Oracle Database 11g), then you can configure it to use Oracle Text 11g as the primary full-text search engine for WebCenter Content. Oracle Text 11g 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 11g, 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.

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.

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.

If you have Oracle Database 11g, 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.

Creating a Search Schema and Configuring an External Data Source

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,
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).

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), 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.

Configuring OracleTextSearch for Content Server in a Configuration File

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.

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
```

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

Extracting and Running the Installation File for 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.

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:

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
```

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.

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 doesn't 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
```

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).

```
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.)

Creating a Hash Partition to Improve Database Performance

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
;
```

E

Updating the JDK After Installing and Configuring an Oracle Fusion Middleware Product

Consider that you have an unsupported JDK version installed on your machine. When you install and configure an Oracle Fusion Middleware product, the utilities, such as Configuration Wizard (`config.sh|exe`), OPatch, or RCU point to a default JDK. The supported JDK version for this release is jdk17.0.12 and it carries security enhancements and bug fixes. You can upgrade the existing JDK to a newer version, and can have the complete product stack point to the newer version of the JDK.

You can maintain multiple versions of JDK and switch to the required version on need basis.

About Updating the JDK Location After Installing an Oracle Fusion Middleware Product

The binaries and other metadata and utility scripts in the Oracle home and Domain home, such as RCU or Configuration Wizard, use a JDK version that was used while installing the software and continue to refer to the same version of the JDK. The JDK path is stored in a variable called JAVA_HOME which is centrally located in .globalEnv.properties file inside the *ORACLE_HOME*`/oui` directory.

The utility scripts such as config.sh|cmd, launch.sh, or opatch reside in the *ORACLE_HOME*, and when you invoke them, they refer to the JAVA_HOME variable located in .globalEnv.properties file. To point these scripts and utilities to the newer version of JDK, you must update the value of the JAVA_HOME variable in the .globalEnv.properties file by following the directions listed in Updating the JDK Location in an Existing Oracle Home .

To make the scripts and files in your Domain home directory point to the newer version of the JDK, you can follow one of the following approaches:

- Specify the path to the newer JDK on the Domain Mode and JDK screen while running the Configuration Wizard.

  For example, consider that you installed Oracle Fusion Middleware Infrastructure with the JDK version 8u191. So, while configuring the WebLogic domain with the Configuration Assistant, you can select the path to the newer JDK on the Domain Mode and JDK screen of the Configuration Wizard. Example: `/scratch/jdk/jdk17.0.12`.

- Manually locate the files that have references to the JDK using `grep` (Linux) or `findstr` (WINDOWS) commands and update each reference.

  See Updating the JDK Location in an Existing Oracle Home .

> **Note:**
>
> If you install the newer version of the JDK in the same location as the existing JDK by overwriting the files, then you don't need to take any action.

Updating the JDK Location in an Existing Oracle Home

The `getProperty.sh|cmd` script displays the value of a variable, such as JAVA_HOME, from the .globalEnv.properties file. The `setProperty.sh|cmd` script is used to set the value of variables, such as OLD_JAVA_HOME or JAVA_HOME that contain the locations of old and new JDKs in the .globalEnv.properties file.

The `getProperty.sh|cmd` and `setProperty.sh|cmd` scripts are located in the following location:

(Linux) *ORACLE_HOME*`/oui/bin`

(Windows) *ORACLE_HOME*`\oui\bin`

Where, *ORACLE_HOME* is the directory that contains the products using the current version of the JDK, such as jdk17.0.12.

To update the JDK location in the .globalEnv.properties file:

1. Use the `getProperty.sh|cmd` script to display the path of the current JDK from the JAVA_HOME variable. For example:

   (Linux) *ORACLE_HOME*`/oui/bin/getProperty.sh JAVA_HOME`

   (Windows) *ORACLE_HOME*`\oui\bin\getProperty.cmd JAVA_HOME`

   ```
   echo JAVA_HOME
   ```

   Where JAVA_HOME is the variable in the .globalEnv.properties file that contains the location of the JDK.

2. Back up the path of the current JDK to another variable such as OLD_JAVA_HOME in the .globalEnv.properties file by entering the following commands:

   (Linux) *ORACLE_HOME*`/oui/bin/setProperty.sh -name OLD_JAVA_HOME -value` *specify_the_path_of_current_JDK*

   (Windows) *ORACLE_HOME*`\oui\bin\setProperty.cmd -name OLD_JAVA_HOME -value` *specify_the_path_of_current_JDK*

   This command creates a new variable called OLD_JAVA_HOME in the .globalEnv.properties file, with a value that you have specified.

3. Set the new location of the JDK in the JAVA_HOME variable of the .globalEnv.properties file, by entering the following commands:

   (Linux) *ORACLE_HOME*`/oui/bin/setProperty.sh -name JAVA_HOME -value` *specify_the_location_of_new_JDK*

   (Windows) *ORACLE_HOME*`\oui\bin\setProperty.cmd -name JAVA_HOME -value` *specify_the_location_of_new_JDK*

   After you run this command, the JAVA_HOME variable in the .globalEnv.properties file now contains the path to the new JDK, such as jdk17.0.12.

Updating the JDK Location in an Existing Domain Home

You must search the references to the current JDK, for example 1.8.0_191 manually, and replace those instances with the location of the new JDK.

You can use the `grep` or `findstr` commands to search for the JDK-related references.

You'll likely be required to update the location of JDK in the following three files:

(Linux) *DOMAIN_HOME*`/bin/setNMJavaHome.sh`

(Windows) *DOMAIN_HOME*`\bin\setNMJavaHome.cmd`

(Linux) *DOMAIN_HOME*`/nodemanager/nodemanager.properties`

(Windows)*DOMAIN_HOME*`\nodemanager\nodemanager.properties`

(Linux) Start `bash` and then run *DOMAIN_HOME*`/bin>source setDomainEnv.sh`

(Windows)*DOMAIN_HOME*`\bin\setDomainEnv.cmd`