Oracle® Fusion Middleware

Installation Guide for Oracle WebCenter Interaction

10*g* Release 4 (10.3.3.0.0) for Unix and Linux

E14548-03

January 2012

Describes how to install Oracle WebCenter Interaction for UNIX and Linux.

ORACLE

Oracle Fusion Middleware Installation Guide for Oracle WebCenter Interaction, 10*g* Release 4 (10.3.3.0.0) for Unix and Linux

E14548-03

Primary Author: Sarah Bernau

Contents

Preface

This book describes how to install and deploy Oracle WebCenter Interaction for UNIX and Linux 10*g* Release 4 (10.3.3.0.0). It is designed to be a quick reference for users with installation experience, while also providing detailed instructions for users installing for the first time.

Audience

This documentation is written for the user responsible for installing this product. This user must have strong knowledge of the platform operating system, database, Web and application servers, and any other third-party software required for installation.

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

For more information, see the following documents in the Oracle WebCenter Interaction 10*g* Release 4 (10.3.3.0.0) documentation set:

- *Oracle WebCenter Interaction Release Notes*
- *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Interaction*
- *Oracle Fusion Middleware User's Guide for Oracle WebCenter Interaction*
- *Oracle Fusion Middleware Deployment Planning Guide for Oracle WebCenter Interaction*
- *Oracle Fusion Middleware User Interface Customization Guide for Oracle WebCenter Framework Interaction*
- *Oracle Fusion Middleware Web Service Developer's Guide for Oracle WebCenter Interaction*

Conventions

The following text conventions are used in this document:

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

Oracle WebCenter Interaction Installer Overview

This chapter provides an overview of the components available in the Oracle WebCenter Interaction installer and the steps necessary to install those components.

1.1 Oracle WebCenter Interaction Components

The Oracle WebCenter Interaction installer includes the following components:

- Portal services and components
  - Administrative Portal

    The administrative portal handles portal setup, configuration, and content. It enables administrative functions, such as creating and managing portlets and other Web services.
  - Automation Service

    The Automation Service runs jobs and other automated portal tasks. You run jobs to perform tasks such as crawling documents into the Knowledge Directory, synchronizing groups and users with external authentication sources, and maintaining the search collection.
  - Portal

    The portal serves end user portal pages and content. It enables end users to access portal content through My Pages, community pages, the Knowledge Directory, and search. The portal also enables some administrative actions, such as setting preferences on portlets or managing communities.
  - API Service

    The API Service provides access to the SOAP API.
  - Image Service

    The Image Service serves static content used or created by portal components. It serves images and other static content for use by the Oracle WebCenter Interaction system.

    Whenever you extend the base portal deployment to include additional components, such as portal servers or integration products, you may have to install additional Image Service files. For information on installing the Image Service files for those components, refer to the documentation included with the component software.

- Search

  The Search component indexes portal content such as documents, portlets, communities, and users as well as many other Oracle WebCenter objects.

- Document Repository Service

  The Document Repository Service stores content uploaded into the portal and Oracle WebCenter Collaboration.

- Content Upload Service

  The Content Upload Service lets you add files to the portal's Knowledge Directory by uploading them to the Document Repository Service, rather than leaving them in their original locations. This is useful if users must access documents located in an internal network from outside your network.

- Directory Service

  The Directory Service enables Oracle WebCenter Interaction to act as an LDAP server, exposing the user, group, and profile data in the portal database through an LDAP interface. This enables other Oracle WebCenter products (and other third-party applications) to authenticate users against the portal database.

- Remote Portlet Service

  The Remote Portlet Service includes the following components:

  * Activity Service

    The Activity Service includes several the User Status portlet and the User Activities portlet. For information on these portlets, see the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Interaction* or the Oracle WebCenter Interaction online help.

    It also includes a REST-based API for submitting activities into a user's activity stream.

    Note: If you use the REST-based API to submit other activities into the activity stream, those activities will also be displayed in the User Activities portlet.

    ---

  * Remote Portlets

    There are several portlets included with the Remote Portlet Service: Enterprise Poke, KD Browser, Last 5 Profile Viewers, My Picture, Online Now, Posted Links, Total Profile Views, RSS Reader, and Submit to KD. For information on these portlets, see the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Interaction* or the Oracle WebCenter Interaction online help.

- Notification Service

  The Notification Service enables the portal to send e-mail notifications to users upon specified events. There are no portal events that trigger notifications, but other Oracle WebCenter events do trigger notifications. For example, Oracle WebCenter Collaboration can be configured to send notifications to users when documents are uploaded.

- Tagging Engine Service

The Tagging Engine is a collaborative information discovery and recovery system that provides personal and collective management of enterprise content, helping you more effectively locate, organize, and share information.

You organize content by using tags, which are meaningful keywords that you and other people create and apply to items and people. If your administrator has enabled the auto-tagging feature, the system automatically tags items and people that fit the auto-tagging criteria.

You can search for items and people by creating search queries that can include a combination of text, tags, and properties.

Included with the Tagging Engine are several portlets to access tagging features: Tagging Engine Items, Tagging Engine People, Tagging Engine Search, Tagging Engine Tag Cloud, and Tagging Engine Results. For information on these portlets, see the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Interaction* or the Oracle WebCenter Interaction online help.

Note: There is also an intrinsic Tag Me portlet that is installed with the portal. This portlet relies on the Tagging Engine for it to function. For information on configuring the Tag Me portlet, see Section A.2, "Configuring the Tag Me Portlet."

  - Search Service

    The Search Service communicates tagging information between the portal, the Tagging Engine, and Oracle WebCenter Collaboration. It performs search queries and returns content to the requesting component (the Tagging Engine or Oracle WebCenter Collaboration).

- Crawler services

  Content Services scan third-party systems/applications for new content, categorizing links to this content in the organized, searchable structure of the portal's Knowledge Directory. Users can then access this content through the portal user interface.

  - Documentum Content Service
  - UCM Content Service

- Identity services

  Identity Services let you import users, groups, and user profile information from third-party user repositories into the portal. Identity Services also enable the portal to authenticate users through the third-party user repositories.

  - LDAP Identity Service

- Development tools

  - Interaction Development Kit (IDK)

    The IDK enables Java and .NET developers to rapidly build, deliver, and enhance user-centric composite applications through Oracle WebCenter Interaction. It provides interfaces for Integration Web Services—authentication, profile, crawler, and search—that integrate enterprise systems into Oracle WebCenter Interaction. It provides SOAP-based remote APIs to expose portal, search, and Oracle WebCenter

Collaboration features. In addition, the IDK has an extensive portlet API to assist in portlet development.

– JSR 168 Container

The Oracle WebCenter JSR-168 Container lets you deploy portlets in Oracle WebCenter Interaction that conform to the JSR-168 portlet standard.

1.1.1 Installation Roadmap

This section provides an overview of the steps necessary to deploy Oracle WebCenter Interaction.

1. Prepare your computers for installation by confirming that you have the required software, users and permissions, environment variables, and such as described in Chapter 2, "Installation Prerequisites."
2. Run the installer as described in Chapter 3, "Installing Oracle WebCenter Interaction."
3. Create and configure the databases used by Oracle WebCenter Interaction as described in Chapter 4, "Creating and Configuring Databases for Oracle WebCenter Interaction."
4. Start the Oracle WebCenter Interaction daemons, run diagnostics scripts to verify your installation, start the portal, and import the portal objects in the migration packages as described in Chapter 5, "Postinstallation Tasks."
5. Perform additional postinstallation for optional components as described in the following appendixes:
   - If you installed the Tagging Engine, complete the tasks described in Appendix A, "Completing Installation of the Tagging Engine."
   - If you installed the Oracle WebCenter Interaction Content Service for Documentum, complete the tasks described in Appendix B, "Completing Installation of Oracle WebCenter Interaction Content Service for Documentum."
   - If you installed the Oracle WebCenter Interaction Content Service for Oracle Universal Content Management, complete the tasks described in Appendix C, "Completing Installation of Oracle WebCenter Content Service for Oracle Universal Content Management."
   - If you installed the Oracle WebCenter Interaction Identity Service for LDAP, complete the tasks described in Appendix D, "Completing Installation of Oracle WebCenter Interaction Identity Service for LDAP."

2

Installation Prerequisites

This chapter provides software requirements, as well as environmental and third-party software prerequisites. You must read this chapter and meet the prerequisites before proceeding to the installation.

Complete the following basic steps to prepare your network and host computers for deployment:

1. Download the most up-to-date documentation from the Oracle Technology Network in the Oracle WebCenter Interaction 10*g* Release 4 (10.3.3.0.0) documentation set.
2. Read the product release notes for information on compatibility issues, known problems, and workarounds that might affect how you proceed with your deployment.
3. Provision host computers for your deployment and install prerequisite software. For details, see Section 2.1, "Software Requirements."
4. Ensure that you have the users and groups required to install Oracle WebCenter Interaction. For details, see Section 2.2, "User and Group Requirements."
5. Grant user and group access rights to Oracle Inventory directories. For details, see Section 2.3, "Granting User and Group Access Rights to Oracle Inventory Directories."
6. If you are installing on AIX, adjust your file size limit and temp directory to accommodate the Oracle WebCenter Interaction installer. For details, see Section 2.4, "Adjusting AIX File Size Limit and Temp Directory."
7. If you are using Oracle Database in your deployment, set the Oracle environment variables. For details, see Section 2.5, "Setting Oracle Environment Variables."
8. If you are using Oracle WebLogic Server in your deployment, disable Basic Authentication. For details, see Section 2.6, "Preparing Oracle WebLogic Server for Oracle WebCenter Interaction."
9. If you are using Tomcat in your deployment, configure the appropriate settings. For details, see Section 2.7, "Preparing Tomcat for Oracle WebCenter Interaction."
10. If you are installing Oracle WebCenter Interaction Content Service for Documentum, you must first install the Documentum DFC Runtime Environment. For details, see Section 2.8, "Configuring the Documentum DFC Runtime Environment."

2.1 Software Requirements

For the latest information on supported operating systems, application servers, databases, and browsers, see the Oracle Fusion Middleware Supported System Configurations page at http://www.oracle.com/technology/software/products/ias/files/fusion_certification.html, open the System Requirements and Supported Platforms for Oracle WebCenter Interaction 10*g*R4 spreadsheet, and refer to the WebCenter Interaction 10.3.3 worksheet.

For more information on recommended configurations based on the size of your implementation, see the section about provisioning computers in the *Oracle Fusion Middleware Deployment Planning Guide for Oracle WebCenter Interaction*.

2.2 User and Group Requirements

This section describes the user and group requirements for Oracle WebCenter products on UNIX and Linux platforms.

We recommend that you create a user and group that will own the portal installation. The following table lists recommended values for a user, a group, and Oracle WebCenter directories.

Are these settings still what we use?

Pre-install Setting	Standard Value	Notes
ALI Group Name	ali	Local group with a fixed ID
ALI User	ali	Local group with a fixed ID
PT_HOME	/opt/oracle/middleware/wci	Owned by ALI user and group

2.2.1 Important Information

The same values for these users, groups, and directories should be used across all computers hosting portal components. Local users and groups with fixed IDs are recommended. Secure deployments should avoid NIS users for computer security. Using the same local user and group for all Oracle WebCenter services allows an administrator to lock down host computers and audit activity.

For convenience, preinstall.sh, a script to create users, groups and directories, is provided with the distribution. For details on running the pre-install script, see Section 2.2.2, "Running the UNIX Pre-Install Script."

You must also grant this user and group access rights to the Oracle Inventory directories. For details, see Section 2.3, "Granting User and Group Access Rights to Oracle Inventory Directories."

2.2.2 Running the UNIX Pre-Install Script

This section describes how to use the pre-install script to create users and groups for Oracle WebCenter Interaction on UNIX and Linux.

The preinstall.sh script creates a user, a group and directories with permissions appropriate for a Oracle WebCenter Interaction installation on UNIX. The script is interactive, asking you a series of questions about the values to be configured.

1. Review the preinstall.sh script.
2. Log in as root to become **superuser**.

3. Make a temporary directory for the files and allow all users to access these files by typing:

   ```
   # mkdir /tmp/plumtree
   ```

   ```
   # chmod 777 /tmp/plumtree
   ```

   Should we still be using plumtree?

4. Copy the preinstall file by typing:

   ```
   # cd /tmp/plumtree
   ```

   ```
   # cp /install_dir/scripts/preinstall.sh .
   ```

5. Run the preinstall.sh script by typing:

   ```
   # ./preinstall.sh
   ```

   Be sure to carefully review any output from the script.

6. Change the password of the newly created user by typing:

   ```
   # passwd ali
   ```

7. Enter the login password.

8. Log out as **superuser**.

2.3 Granting User and Group Access Rights to Oracle Inventory Directories

Oracle Inventory includes files that provide the Oracle Universal Installer with the locations of the ORACLE_HOME directories on a particular computer. For Oracle Inventory to function properly, the user that installs Oracle WebCenter Interaction must have access rights to the directories that contain Oracle Inventory's files. You can set the user and group access rights for these directories by running the ouais.sh shell script.

1. Log in to the remote server host computer as the root user.

2. Copy the ouais.sh script to the computer onto which you will be installing Oracle WebCenter Interaction.

   This script is located in the same location as the Oracle WebCenter Interaction installer file.

3. Change the current directory (`cd`) to be the directory to which you copied the ouais.sh script.

4. Run the ouais.sh shell script.

   As arguments to the script, specify the ALI user and group you created that will run the Oracle WebCenter Interaction installer. For details, see Section 2.2, "User and Group Requirements." For example, you would use the following command to run the ouais.sh script from the root shell:

   ```
   ./ouais.sh -u <oracleuser> -g <oraclegroup>
   ```

   The ouais.sh script creates the Oracle Inventory directory if it did not exist before you ran the script. Additionally, the script grants user and group ownership to the directories that contain the files that are used by Oracle Inventory.

2.4 Adjusting AIX File Size Limit and Temp Directory

If you are installing on AIX, adjust your file size limit and temp directory to accommodate the Oracle WebCenter Interaction installer.

1. View your local default values, using the following command:

   ```
   $ulimit -a
   ```

   By default, AIX limits the maximum size of files to 1GB. The default value is set to 2097151 in the /etc/security/limits file, but the value is in 512byte blocks, so it might look like the limit is 2GB when it is really only 1GB.

2. If your limit is less than 2GB (approximately 4194304 in 512btye blocks), adjust the limit as root (only root can adjust limits upward):

   ```
   $ulimit -f 4194304
   ```

3. For the change to take effect, you must log out and log back in.

4. The default temp location (/tmp) will not accommodate the space needed for the Oracle WebCenter Interaction installer extraction process, so you must define a different location for the extracted files by setting the following variable, pointing to a new temp directory:

   ```
   export IATEMPDIR="new_temp_directory"
   ```

2.5 Setting Oracle Environment Variables

This table describes the Oracle Environment variables that must be set when installing Oracle WebCenter products to instances of Oracle9*i* or Oracle Database 10*g*.

Environment Variable	Description	Example Values
ORACLE_BASE	Must be set to the *root* directory of your Oracle installation.	▪ /opt/oracle
ORACLE_HOME	Must be set to the *home* directory of your Oracle installation.	▪ /opt/oracle/ora92
ORACLE_SID	Must be set to the system ID (SID) of the portal database instance.	▪ (Oracle9*i*) PLUM ▪ (Oracle Database 11*g*) PLUM11 **Note**: PLUM or PLUM10 are expected by the SQL scripts. If you set your SID to a value other than these example values, you must edit the SQL scripts to reflect this change.

2.6 Preparing Oracle WebLogic Server for Oracle WebCenter Interaction

This section describes how to configure Oracle WebLogic Server for use with the Oracle WebCenter Interaction portal application.

WebLogic Basic Authentication must be disabled for the Oracle WebCenter Interaction portal application on Oracle WebLogic Server. To do this, in the Oracle WebLogic Server config.xml for the Oracle WebCenter Interaction portal, set `<enforce-valid-basic-auth-credentials>` to `false`.

1. Disable WebLogic Basic Authentication for the Oracle WebCenter Interaction portal application.

a. Open *WebLogic_home*/user_projects/domains/*domain*/config/config.xml in a text editor, where *WebLogic_home* is your Oracle WebLogic installation directory.

b. In the `<security-configuration>` section, set `<enforce-valid-basic-auth-credentials>` to `false`.

   If `<enforce-valid-basic-auth-credentials>` is already defined in this section, change its value to `false`.

   If `<enforce-valid-basic-auth-credentials>` does not exist in this section, add the following line before the `</security-configuration>` line as shown below:

```
<security-configuration>
...
    <enforce-valid-basic-auth-credentials>
    false
    </enforce-valid-basic-auth-credentials>
</security-configuration>
```

2. On Oracle Enterprise Linux, AIX, HP-UX, and Solaris, verify that your Oracle WebLogic Server domain is configured to use a valid 64–bit Java SDK.

3. On Oracle Enterprise Linux, AIX, HP-UX, and Solaris, add `-d64` to your domain's JAVA_OPTIONS.

   To do this, edit the setDomainEnv.sh script for your domain. Find where `JAVA_OPTIONS` is set, near the end of the file, and add the `-d64` flag.

   For example:

```
#JAVA_OPTIONS="${JAVA_OPTIONS}"
JAVA_OPTIONS="-d64 ${JAVA_OPTIONS}"
export JAVA_OPTIONS
```

4. Increase the JVM's `MaxPermSize`.

   A `MaxPermSize` of `256m` is recommended. If `MaxPermSize` is set too low, you will see `java.lang.OutOfMemoryError: PermGen space` when attempting to start the portal.To increase `MaxPermSize`, edit the `setDomainEnv.sh` script for your domain. Find where `MaxPermSize` is being set for your `JAVA_VENDOR`, and set it to `256m`.

   For example:

```
if [ "${JAVA_VENDOR}" = "HP" ] ; then
    #MEM_ARGS="${MEM_ARGS} -XX:MaxPermSize=128m"
    MEM_ARGS="${MEM_ARGS} -XX:MaxPermSize=256m"
    export MEM_ARGS
fi
```

2.7 Preparing Tomcat for Oracle WebCenter Interaction

This section describes configuration of Tomcat required before the installation and deployment of Oracle WebCenter Interaction.

1. Create the directory tomcat_home/conf/Catalina/localhost, if necessary.

   On a fresh install of Tomcat 6.0, this directory might not exist. If the directory does not exist, you must create it.

2. On AIX, HP-UX, and Solaris, verify that Tomcat is configured to use a valid 64–bit Java SDK.
3. On AIX, HP-UX, and Solaris, add `-d64` to Tomcat's Java options.

   To do this, edit your Tomcat catalina.sh script. Add `-d64` to the `JAVA_OPTS` environment variable.

   For example:

```
JAVA_OPTS="-d64 ${JAVA_OPTS}"
Export $JAVA_OPTS
```

2.8 Configuring the Documentum DFC Runtime Environment

If you are installing Oracle WebCenter Interaction Content Service for Documentum, you must first install the Documentum DFC Runtime Environment. For details on installation of Documentum products, refer to Documentum documentation.

After you install the Documentum Desktop Client on the Remote Server host computer, configure the dmcl.ini file for the client as follows:

- Set the host to the docbroker that will be used by all users of this Remote Server. To allow more than one docbroker, you must install a Remote Server for each docbroker.

```
[DOCBROKER_PRIMARY]
host = YOURDOCBROKER
```

- Set your max session count to a value comfortably above the number of sessions you expect to be opened by the Oracle WebCenter Interaction Content Service for Documentum content Web services (1 connection per user per content Web service) but comfortably within this computer's performance limitations and well below the maximum number of concurrent sessions allowed by your Documentum server. For more information, refer to Section B.8, "Advanced Configuration: Tuning Documentum Server."

```
[DMAPI_CONFIGURATION]
cache_query = T
connect_pooling_enabled=T
connect_recycle_interval=100
max_session_count=
Docbroker_search_order=RANDOM
```

2.8.1 Additional Step for UNIX and Linux Hosts

Ensure you have set environment variables for any user who uses this DFC instance by adding them to the Java application server startup file:

- **DOCUMENTUM**: refer to the DFC Installation Guide.
- **DOCUMENT_SHARED**: refer to the DFC Installation Guide.
- **CLASSPATH**: include full path to dfc.jar, dctm.jar, and $DOCUMENTUM_SHARED/config. For example:

```
export CLASSPATH=$CLASSPATH:/user/DFC/dfc.jar:$DOCUMENTUM_
SHARED/dctm.jar:$DOCUMENTUM_SHARED/config
```

- **LD_LIBRARY_PATH** (Solaris and Linux): include the full path to the dfc directory under the Documentum DFC program root. Add the full path to the dfc directory to LD_LIBRARY_PATH. For example

```
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/documentum_dfc_program_root/dfc
```

- **LIBPATH** (AIX): include the full path to the dfc directory under the Documentum DFC program root. Add the full path to the dfc directory to LIBPATH. For example:

  ```
  export LIBPATH=$LIBPATH:/documentum_dfc_program_root/dfc
  ```

- **PATH**: enter the full path to the installation directory.
- **DMCL_CONFIG**: enter the path to a dmcl.ini file. For example:

  ```
  export DMCL_CONFIG=/user/DFC/dmcl.ini
  ```

> **Note:** We strongly recommend that you set the DMCL_CONFIG system variable on the Remote Server to ensure that the Oracle WebCenter Interaction Content Service for Documentum can communicate with the Documentum server. The DMCL_CONFIG value should be the path to the dmcl.ini file. See the installation guide for Documentum DFC Runtime Environment for additional details.

3

Installing Oracle WebCenter Interaction

This chapter describes how to complete the Oracle WebCenter Interaction installer wizard and how to deploy the portal application and Image Service to your application server.

3.1 Installing the Oracle WebCenter Interaction Components

This section describes how to run the Oracle WebCenter Interaction installer. Before installing Oracle WebCenter Interaction you must complete the tasks described in Chapter 2, "Installation Prerequisites."

1. Log in to the host as the ALI user.
2. Close all programs.
3. Launch the Oracle WebCenter Interaction installer.

   The installer file is named WebCenterInteraction_10.3.3.0.0. The Oracle WebCenter Interaction installer is a graphical, X-Windows client when run in interactive mode. If you run the installer on a remote terminal, ensure that your DISPLAY is set appropriately.
4. Complete the installer wizard pages.

   For details, see Section 3.2, "Oracle WebCenter Interaction Installer Wizard Pages"
5. Configure environment settings for Oracle WebCenter Interaction.

   Source the script *install_dir*/pthome.sh in the startup script for your application server. The pthome.sh script sets up the environment for Oracle WebCenter components.
6. Deploy the portal application to your application server.

   The portal Web application archives are located in *install_dir*/ptportal/10.3.3/webapp/.

   - If you are deploying to Tomcat, deploy portal.war.
   - If you are deploying to Oracle WebLogic Server or IBM WebSphere, deploy portal.ear.
7. Deploy the Image Service to your application server.

   The Image Service files are located in *install_dir*/ptimages/imageserver/.

   For instructions, see Section 3.3, "Deploying the Image Service."

3.2 Oracle WebCenter Interaction Installer Wizard Pages

This section describes the Oracle WebCenter Interaction installer wizard pages.

Wizard Page	Description
Introduction	This installer wizard page provides a brief description of the installer and describes how to run the installer in silent mode.
Installation Folder	Accept the default installation folder or select a different folder in which to install Oracle WebCenter Interaction. Default: /opt/oracle/middleware/wci
Choose Components	Select either **Complete** or **Custom**. If you select **Complete**, a full set of Oracle WebCenter Interaction components is installed. If you select **Custom**, you can select individual portal components to install according to your deployment plan.
Configuration Manager - Port and Password	Enter the port and password for the Configuration Manager Web tool. The Configuration Manager will be used to complete the installation of Oracle WebCenter Interaction.
Standalone or Cluster	Select whether you would like to install a **Single Standalone Search Node** or add a **Search Cluster Node**. Selecting to install the standalone search node installs a single node on the local computer. If you want to support failover, add search cluster nodes.
Adding New Search Node	Enter the name and port number of the new search node. The search node is installed into *install_dir*/ptsearchserver/10.3.3.
Search Cluster Files	If you chose to install a search cluster node, select the location of the search cluster files. You must have permission to access and write to the location where you want to install these files. Example: *install_dir*/ptsearchserver/10.3.3/cluster
Content Service for Documentum - Application Port	Choose whether to use a secure protocol (https) for the Oracle WebCenter Interaction Content Service for Documentum or a standard protocol (http). Specify your port number. The default port is 11951. Make sure to enter the SSL port number if using https.
Documentum Client Library	Enter the path to your Documentum client library. Example: `$DOCUMENUM_SHARED/dfc/dfcbase.jar`
Fully Qualified Domain Name	Enter the fully qualified domain name for the computer hosting Oracle WebCenter Interaction Content Service for Windows Files.
Identity Service for LDAP - Application Port	Choose whether to use a secure protocol (https) for the Oracle WebCenter Interaction Identity Service for LDAP or a standard protocol (http). Specify your port number. The default port is 11950. Make sure to enter the SSL port number if using https.
Fully Qualified Domain Name	Enter the fully qualified domain name for the computer hosting Oracle WebCenter Interaction Identity Service for Microsoft Active Directory.
Interaction Development Kit: .NET Signed or Unsigned	Choose whether to install the .NET signed or unsigned version of the Oracle WebCenter Interaction Development Kit (IDK).
Fully Qualified Domain Name	Enter the fully qualified domain name for the computer hosting Oracle WebCenter Console for Microsoft SharePoint.
Pre-Installation Summary	Review the list of components to be installed. Click **Install**.

Wizard Page	Description
Launch Configuration Manager	Launch the Configuration Manager. The Configuration Manager is located at: `https://host:port` Where *host* is the host you are installing on and *port* is the port you specified. Log in to the Configuration Manager using the user name `administrator` and the password you specified on the Configuration Manager – Port and Password page. The Configuration Manager displays a list of all recently installed components. Clicking the link next to each component leads you through the settings you must configure to complete the installation. For information on the settings in the Configuration Manager, refer to the Configuration Manager online help or to the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Interaction*. When you have completed all Configuration Manager tasks, return to the installer.
Application Settings Confirmation	Choose whether you have completed configuration of your application settings or want to complete configuration later.
Install Complete	When the installer is finished, you might be asked to restart your computer to complete installation. If prompted, choose whether to restart your computer now or manually at another time. Click **Done**. **Note:** The Oracle WebCenter Interaction installer launches additional installers depending on the components you chose to install. You might be prompted by one of the additional component installers to restart your computer before the Oracle WebCenter Interaction installer is finished. If you are prompted to restart your computer while another installer is running, select the option to manually restart your computer later. Then, if you are not prompted to restart your computer after the final installer is finished, restart your computer manually.

3.3 Deploying the Image Service

The Image Service is a collection of static, non-secure files that should be served by an HTTP server, such as Apache HTTP Server. The Image Service files are located in *install_dir*/ptimages/imageserver.

This directory should be aliased in your HTTP server configuration so that the URL specified for the Image Service when the installer was run is correct. For example, if you were running an Apache HTTP Server on port 8082, and you had specified http://webserver:8082/imageserver as your Image Service URL, you might configure Apache HTTP server as follows:

> **Note:** This is only an example. In a production environment the imageserver directory should be aliased to the Web server by a knowledgeable Web server administrator.

1. In a text editor, open the file *Apache_home*/conf/httpd.conf.
2. Alias your *install_dir*/ptimages/imageserver directory to /imageserver/ on the Web server by adding the following alias to the httpd.conf file:

```
Alias /imageserver/ "install_dir/ptimages/imageserver/"
```

3. Create a Directory entry for the imageserver directory:

```
<Directory "install_dir/ptimages/imageserver">
Options Indexes MultiViews
AllowOverride None
Order allow,deny
Allow from all
</Directory>
```

4. Include the bea.conf file you will create next.

```
Include conf/bea.conf
```

5. Save httpd.conf and exit the text editor.
6. In the same folder as the httpd.conf, create a bea.conf file with the following contents, replacing *wls-hostname* and *wls-port* with the actual host name and port number:

```
LoadModule weblogic_module     lib/mod_wl_22.so
# the local weblogic setup
<IfModule mod_weblogic.c>
  WebLogicHost wls-hostname
  WebLogicPort wls-port
  MatchExpression /portal/*
</IfModule>
```

7. From the wls_server installed location, copy mod_wl_22.so to the corresponding app server lib folder (for example, for http server, copy to /usr/local/apache2/lib).
8. Verify /opt/oracle/middleware/wci/ptimages/imageserver is readable by Apache HTTP Server:

```
$ chmod a+r /opt
$ chmod a+r /opt/oracle
$ chmod a+r /opt/oracle/middleware/wci
$ chmod a+r /opt/oracle/middleware/wci/ptimages
$ chmod -R a+r /opt/oracle/middleware/wci/ptimages/imageserver
```

9. When Apache HTTP Server is restarted, http://webserver:8082/imageserver/ should point to *install_dir*/ptimages/imageserver/.

4

Creating and Configuring Databases for Oracle WebCenter Interaction

This chapter describes how to create and configure the portal, Notification Service, and Tagging Engine databases for Oracle WebCenter Interaction.

It includes the following sections:

4.1 Creating and Configuring the Portal Database

This section describes how to create and configure the portal database. It includes the following sections:

4.1.1 Creating and Configuring the Portal Database on Oracle Database for UNIX

This section describes how to create and configure the Oracle WebCenter Interaction portal database on Oracle Database for UNIX.

Notes:

- When running Oracle WebCenter Interaction with Oracle Database 11*g* with the provided initPLUM10.ora file, make the following modification: change `compatible = 10.2.0.0.0` to `compatible = 11.0.0`.
- To prevent problems with "group by" optimizations when using Oracle WebCenter Interaction with Oracle Database 11*g* you must add the following configuration to the bottom of your init$ORACLE_SID.ora file: `_optimizer_group_by_placement=false`.

1. Verify that the Oracle environment variables are properly set.

   For details, see Section 2.5, "Setting Oracle Environment Variables".

2. Copy the SQL scripts from the Oracle WebCenter Interaction installation directory to your Oracle server.

- For Oracle9*i*, the Oracle WebCenter Interaction installer creates the SQL scripts in the following directories:

  ```
  install_dir/ptportal/10.3.3/sql/oracle_unix9.2
  install_dir/aluidirectory/1.1/sql/oracle
  ```

- For Oracle Database 10*g*, the Oracle WebCenter Interaction installer creates the SQL scripts in the following directories:

  ```
  install_dir/ptportal/10.3.3/sql/oracle_unix10
  install_dir/aluidirectory/1.1/sql/oracle
  ```

- For Oracle Database 11*g*, the Oracle WebCenter Interaction installer creates the SQL scripts in the following directories:

  ```
  install_dir/ptportal/10.3.3/sql/oracle_unix11
  install_dir/aluidirectory/1.1/sql/oracle
  ```

3. Configure the portal database, tablespace, and user:
   - If you are creating a new Oracle9*i* database for the Oracle WebCenter Interaction schema, see Section 4.1.1.1, "Creating the Portal Database on Oracle9i for UNIX."
   - If you are creating a new Oracle Database 10*g* or 11*g* for the Oracle WebCenter Interaction schema, see Section 4.1.1.2, "Creating the Portal Database on Oracle Database 10g or 11g for UNIX."
   - If you are creating the Oracle WebCenter Interaction tablespace and schema within an existing Oracle database, see Section 4.1.1.3, "Creating the Portal Tablespace on Oracle Database for UNIX."
4. Create the portal schema and initialize the portal database.

   For details, see Section 4.1.1.4, "Creating the Portal Schema on Oracle Database for UNIX."

4.1.1.1 Creating the Portal Database on Oracle9*i* for UNIX

This section describes how to create and configure the portal database, tablespace, and user on Oracle9*i*.

Note: These steps create a new, dedicated portal database. If you are creating the portal tablespace within an existing database, see Section 4.1.1.3, "Creating the Portal Tablespace on Oracle Database for UNIX."

The following must be done before scripting the database:

- Log in to the portal database host computer as the owner of the Oracle system files.
- Verify that `ORACLE_BASE`, `ORACLE_HOME`, and `ORACLE_SID` are set appropriately. For details, see Section 2.5, "Setting Oracle Environment Variables."
- If this is a re-creation of a database or a retry of a prior failed attempt, delete the old database file.

1. Create and configure the portal database:
   a. Create the `sys` password.

For example: `$ $ORACLE_HOME/bin/orapwd file=$ORACLE_HOME/database/orapwPLUM password=password`

b. Create the PLUM directory under $ORACLE_BASE/oradata.

c. Create a link to initPLUM.ora in $ORACLE_HOME/database.

2. Create the portal database instance:

a. From $ORACLE_BASE/admin/$ORACLE_SID/plumtreescripts, start sqlplus using the `/nolog` parameter.

b. Run the crdb1_oracle_UNIX.sql script to create and start the new database instance.

This script should generate no errors. Output from the script is saved in the file crdb1.lst in the plumtree scripts directory.The database should now be running.

c. Verify that the correct data files have been created.

In $ORACLE_BASE/oradata/$ORACLE_SID you should see the following:

```
systPLUM.dbf
undo1A.dbf
temp1A.dbf (single disk installation only.)
```

3. Create the portal tablespace and user:

a. Run the crdb2_oracle_UNIX.sql script to create tablespaces, create the portal database user, and perform low level database tuning.

This script can take a significant amount of time to complete. The following errors might be generated:

```
ORA-00942 table or view does not exist
ORA-1432/ORA-1434 public synonym to be dropped does not exist
```

These errors are acceptable. Any other errors are not acceptable. Output from the script is saved in the file crdb1.lst in the plumtree scripts directory.

b. Verify that the correct data files have been created.

In $ORACLE_BASE/oradata/$ORACLE_SID you should see the following:

```
PLUMtbl1.dbf
PLUMtmp1.dbf
PLUMidx1.dbf (single disk installation only.)
```

4.1.1.2 Creating the Portal Database on Oracle Database 10*g* or 11*g* for UNIX

This section describes how to create and configure the portal database, tablespace, and user on Oracle Database 10*g* or 11*g*.

> **Note:** These steps create a new, dedicated portal database. If you are creating the portal tablespace within an existing database, see Section 4.1.1.3, "Creating the Portal Tablespace on Oracle Database for UNIX."

The following must be done before scripting the database:

- Log in to the portal database host computer as the owner of the Oracle system files.

- Verify that ORACLE_BASE, ORACLE_HOME, and ORACLE_SID are set appropriately. For details, see Section 2.5, "Setting Oracle Environment Variables."
- If this is a re-creation of a database or a retry of a prior failed attempt, delete the old database file.

1. Create and configure the portal database:
   a. Create the sys password.

      For example: `$ $ORACLE_HOME/bin/orapwd file=$ORACLE_HOME/database/orapwPLUM10 password=password`

   b. Create the PLUM10 directory under $ORACLE_BASE/oradata.

   c. Create a link to initPLUM10.ora in $ORACLE_HOME/database.
2. Create the portal database instance:
   a. From $ORACLE_BASE/admin/$ORACLE_SID/plumtreescripts, start sqlplus using the /nolog parameter.

   b. Run the crdb1_oracle_UNIX.sql script to create and start the new database instance.

      This script should generate no errors. Output from the script is saved in the file crdb1.lst in the plumtree scripts directory. The database should now be running.

   c. Verify that the correct data files have been created.

      In $ORACLE_BASE/oradata/$ORACLE_SID you should see the following:

      ```
      systPLUM10.dbf
      undo1A.dbf
      temp1A.dbf (single disk installation only.)
      ```
3. Create the portal tablespace and user:
   a. Run the crdb2_oracle_UNIX.sql script to create tablespaces, create the portal database user, and perform low level database tuning.

      This script can take a significant amount of time to complete. The following errors may be generated:

      ```
      ORA-00942 table or view does not exist
      ORA-1432/ORA-1434 public synonym to be dropped does not exist
      ```

      These errors are acceptable. Any other errors are not acceptable. Output from the script is saved in the file crdb1.lst in the plumtree scripts directory.

   b. Verify that the correct data files have been created.

      In $ORACLE_BASE/oradata/$ORACLE_SID you should see the following:

      ```
      PLUM10tbl1.dbf
      PLUM10tmp1.dbf
      PLUM10idx1.dbf (single disk installation only.)
      ```

4.1.1.3 Creating the Portal Tablespace on Oracle Database for UNIX

This section describes how to create and configure the portal tablespace and user.

> **Note:** These steps create the portal tablespace within an existing database. If you are creating a new, dedicated portal database, see Section 4.1.1, "Creating and Configuring the Portal Database on Oracle Database for UNIX."

The following must be done before scripting the database:

- Log in to the portal database host computer as the owner of the Oracle system files.
- Verify that `ORACLE_BASE`, `ORACLE_HOME`, and `ORACLE_SID` are set appropriately. For details, see Section 2.5, "Setting Oracle Environment Variables."

1. Connect to your database as a user with sysdba rights.
2. Create the portal tablespace and DB user:
   a. From $ORACLE_BASE/admin/$ORACLE_SID/plumtreescripts, start sqlplus using the `/nolog` parameter.
   b. Run the create_ali_tablespace_UNIX.sql script to create the portal tablespace.
   c. Run the create_ali_user_oracle.sql script to create the portal schema user.

4.1.1.4 Creating the Portal Schema on Oracle Database for UNIX

before creating the portal schema you must configure the database, tablespace, and database user. For details on Oracle9*i*, see Section 4.1.1.1, "Creating the Portal Database on Oracle9i for UNIX." For details on Oracle Database 10*g* or 11*g*, see Section 4.1.1.2, "Creating the Portal Database on Oracle Database 10g or 11g for UNIX."

This section describes how to create the portal schema.

1. If your imageserver is located on a computer than the one hosting your portal server, use a text editor to edit the postinst_oracle.sql file to correctly reflect the imageserver location. Find the following setting, and replace *`server`* with the new location:

   ```
   UPDATE PTOBJECTPROPERTIES SET PROPERTIES2 = '<S
   N="URL">http://server/imageserver/</S></PTBAG>'
   WHERE OBJECTID = 30 AND CLASSID = 48 AND PAGENUMBER = 0
   ```

2. Create the Oracle WebCenter Interaction tables, indexes, and stored procedures.

   Create the Oracle WebCenter Interaction tables, indexes, and stored procedures by running the init_ali_db_oracle.sql script. You must run this script as the portal database user that you created.

   Output from the script is saved in the following files in the scripts directory:

   - create_tables_oracle.lst
   - stored_procs_oracle.lst
   - load_seed_info.lst
   - postinst.lst

3. (Optional) Create an Oracle SPFILE.

   For the benefits of using an SPFILE, refer to Oracle documentation. To create the SPFILE, run the create_spfile_oracle_UNIX.sql script.

4. Create the ALUI Directory tables.

Run the following scripts in order:

a. create_tables.sql

b. create_functions.sql

c. map_alidb_65.sql

4.2 Creating and Configuring the Notification Service Database

This section describes the database configuration options for the Notification service.

By default, the Notification service uses an internal database. If your deployment requires a more robust database, you can configure Notification to use an external database.

To configure an external database:

1. Script your database. For details on scripting an Oracle database, see Section 4.2.1, "Creating an External Notification Database on Oracle Database."
2. Update Notification database configuration information in Configuration Manager.

   The Notification database configuration is located in Configuration Manager under Notification Service | External Database. Details of the necessary settings are provided as inline documentation in the Configuration Manager.

4.2.1 Creating an External Notification Database on Oracle Database

This section describes how to create and configure a database for the Notification service on all supported versions of Oracle Database.

- Log in to the portal database host computer as the owner of the Oracle system files. Unless otherwise noted, scripts must be run as the system user.
- Verify that `ORACLE_BASE`, `ORACLE_HOME`, and `ORACLE_SID` are set appropriately. For details, see Section 2.5, "Setting Oracle Environment Variables."

The script files referred to in the following steps are found in *install_dir*/cns/1.1/sql/oracle/unix. In this directory there are two subdirectories:

1. Edit references to the `PLUM10` SID in cns-server-create-table-space.sql, if necessary.

   The cns-server-create-table-space.sql script assumes your SID to be `PLUM10`. If your SID is different, replace all occurrences of `PLUM10` in the script file with your SID.
2. Run cns-server-create-table-space.sql.
3. Set user and password values in cns-server-create-user.sql.

   In the cns-server-create-user.sql script replace the tokens *@CNSDB_LOGIN@* and *@CNSDB_PASSWORD_UNENCRYPTED@* with the user name and password, respectively, for the user you are creating.
4. Run cns-server-create-user.sql.
5. As the user you just created, run cns-createTables.sql.
6. As the user you just created, run cns-data.sql.

4.3 Creating and Configuring the Tagging Engine Database

This section describes how to create and configure a database for the Tagging Engine.

You only must perform this procedure if you installed the Tagging Engine.

4.3.1 Creating and Configuring the Tagging Engine Database on Oracle Database

To create and configure the Tagging Engine database on Oracle Database:

1. Copy the oracle directory from *install_dir*/pathways/10.3.3/sql/oracle/unix to the Tagging Engine database's host computer. This folder includes the scripts that you will use to set up and configure the Tagging Engine database.
2. Log on to the host computer for the Tagging Engine database as owner of the Oracle system files.
3. Execute the following steps as the system user in your Oracle Database:
   a. Run the script create_pathways_tablespaces.sql for your platform. This file is located in a platform specific subdirectory within the oracle directory that you copied in step 1.

      Note: Before running the script, determine the name of the SID used in your portal database. If necessary, edit the script so that all SID name instances in the script match the SID name used for the portal database.

   b. Run the script create_pathways_user.sql.
4. Execute the following steps as the Tagging Engine user that you just created:
   a. Run the script create_pathways_schema.sql. This script creates all of the tables and indexes that are necessary to run the Tagging Engine. The create_pathways_schema.sql script is located in the oracle directory that you copied in step 1.
   b. Run the script install_pathways_seeddata.sql. This script adds all of the initial seed data that are necessary to run the Tagging Engine. The install_pathways_seeddata.sql script is located in the oracle directory that you copied in step 1.
5. Run your database's analysis tool on the portal database to increase the efficiency of the database.

4.4 Creating and Configuring the ALUI Security Database

This section describes how to set up the ALUI Security database.

Note: You do not must perform this procedure if Oracle WebCenter Analytics is installed. Installing Oracle WebCenter Analytics requires creating the ALUI Security database.

4.4.1 Creating and Configuring the ALUI Security Database on Oracle Database

This section describes how to create and configure the ALUI Security database on Oracle Database.

1. On the computer on which you installed the Tagging Engine, copy the oracle directory from *install_dir*/pathways/10.3.3/sql/oracle/unix to the ALUI Security database's host computer.
2. Log on to the host computer for the ALUI Security database as owner of the Oracle system files.
3. Create the ALUI Security database tablespace.
4. Create the ALUI Security database user.
5. Connect to the ALUI Security database as the ALUI Security database user.
6. Run the create_security_tables.sql script, located in the folder that you copied in step 1.
7. Run your database's analysis tool on the ALUI Security database to the efficiency of the database.

5
Postinstallation Tasks

This chapter describes the tasks you must complete after you install and start Oracle WebCenter Interaction:

1. Starting the Oracle WebCenter Interaction Daemons
2. Running the Diagnostics Script
3. Starting the Portal
4. Importing Migration Packages

If you installed optional components, you might also must perform additional postinstallation as described in the following appendixes

- If you installed the Tagging Engine, complete the tasks described in Appendix A, "Completing Installation of the Tagging Engine."
- If you installed the Oracle WebCenter Interaction Content Service for Documentum, complete the tasks described in Appendix B, "Completing Installation of Oracle WebCenter Interaction Content Service for Documentum."
- If you installed the Oracle WebCenter Interaction Content Service for Oracle Universal Content Management, complete the tasks described in Appendix C, "Completing Installation of Oracle WebCenter Content Service for Oracle Universal Content Management."
- If you installed the Oracle WebCenter Interaction Identity Service for LDAP, complete the tasks described in Appendix D, "Completing Installation of Oracle WebCenter Interaction Identity Service for LDAP."

5.1 Starting the Oracle WebCenter Interaction Daemons

This section describes how to start the daemons associated with Oracle WebCenter Interaction components and the order in which they must be started. Depending on which components you installed, some daemons might not be applicable to your portal installation.

1. Start the Search daemon by executing *install_dir*/ptsearchserver/10.3.3/bin/searchserverd.sh start.
2. Start the Search Cluster Manager daemon by executing *install_dir*/ptsearchserver/10.3.3/adminui/bin/clusterui.sh start.
3. Start the API daemon by executing *install_dir*/ptws/10.3.3/bin/apiserviced.sh start.
4. Start the LDAP Directory daemon by executing *install_dir*/aluidirectory/1.1/bin/ldapserverd.sh start.

5. Start the Automation daemon by executing *install_dir*/ptportal/10.3.3/bin/automationserverd.sh start.
6. Start the Notification daemon by executing *install_dir*/cns/1.1/bin/cnsd.sh start.
7. Start the Document Repository daemon by executing *install_dir*/ptdr/10.3.3/bin/drserverd.sh start.
8. Start the Console Logger daemon by executing *install_dir*/ptlogging/10.3.3/bin/ptlogger.sh start.
9. Start the Configuration Manager daemon by executing *install_dir*/configmgr/2.1/bin/configmgr.sh start.
10. Start the Content Upload daemon by executing *install_dir*/ptupload/10.3.3/bin/contentuploadd.sh start.
11. Start the Tagging Engine daemon by executing *install_dir*/pathways/10.3.3/bin/pathwaysserverd.sh start.
12. Start the Search Service daemon by executing *install_dir*/searchservice/1.2/bin/searchserviced.sh start.
13. Start the Remote Portlet daemon by executing *install_dir*/remoteps/1.1/bin/remotepsd.sh start.
14. Start the Content Service for Documentum by executing *install_dir*/dctmcws/10.3.3/bin/dctmcsd.sh start.
15. Start the Content Service for UCM daemon by executing *install_dir*/ptucmcws/10.3.3/bin/ucmcwsd.sh start.
16. Start the Identity Service for LDAP daemon by executing *install_dir*/ptldapaws/10.3.3/bin/ldapawsd.sh start.

5.2 Running the Diagnostics Script

This section describes how to use the diagnostics script to determine the health of your Oracle WebCenter Interaction installation before running the portal for the first time.

before running the diagnostics script, you must completely configure Oracle WebCenter Interaction using the Configuration Manager. You must also create and configure the portal database.

Run the diagnostics script before starting your portal for the first time. It tests basic portal startup functionality. If there are issues with your Oracle WebCenter Interaction installation, the diagnostics script generates a list of warnings and recommendations about how to correct the issues. Run the script, follow the recommendations, and correct any issues before starting your portal for the first time.

- Run the diagnostics script, *install_dir*/ptportal/10.3.3/bin/diagnostic.sh

> **Note:** If the diagnostics script fails, run *install_dir*/ptportal/10.3.3/bin/ptverify.sh and review any issues it discovers.

5.3 Starting the Portal

This section describes how to start the Oracle WebCenter Interaction portal for the first time.

To start the portal:

1. Start the portal by browsing to the server.pt application at the external portal URL you provided the Oracle WebCenter Interaction installer.

   For example, `http://myportal.domain.com:80/portal/server.pt`

2. Log in to the portal as Administrator with no password.

> **Note:** You should change the default Administrator password as soon as possible. Ensure that you document the change and inform the appropriate portal administrators.

5.4 Importing Migration Packages

This section provides an overview of how to import the Oracle WebCenter Interaction component migration packages. Depending on which components you installed, some packages might not be applicable to your portal installation.

Use the Migration - Import Utility (click **Administration**, then **Select Utility**, then **Migration - Import**) to import the migration packages.

If necessary, adjust any import settings. For details on using the Migration - Import utility, see the online help or *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Interaction*.

Import the migration packages relevant to your installation:

- Import the Search Cluster Manager, import the migration package located in *install_dir*/ptsearchserver/10.3.3/serverpackages:
  - SearchClusterAdminUI.pte

> **Note:** You might must log out and back in to the portal to see the **Search Cluster Manager** option in the **Select Utility** menu.

- If you installed the Content Upload service, import the migration package located in *install_dir*/ptupload/10.3.3/serverpackages:
  - contentupload.pte
- If you installed the Remote Portlet Service, import the migration packages located in *install_dir*/remoteps/1.1/serverpackages:
  - activityservice.pte
  - EnterprisePoke.pte
  - KnowledgeDirectoryPortlet.pte
  - MyPictureProfilePortlet.pte
  - PostedLinksPortlet.pte
  - ProfilePortlets.pte
  - RSSReader.pte
  - RSSContentTypesAndProperties.pte
  - RSSTypeMapAndPropertyMap_Global.pte

- If you installed the Notification service, import the migration package located in *install_dir*/cns/1.1/serverpackages:
  - notification.pte
- If you installed the Tagging Engine, import the migration packages located in *install_dir*/pathways/10.3.3/serverpackages:
  - TaggingEngine.pte
  - TaggingEngine_autotag_ext_op.pte

    This package add a job for automatically tagging objects in the Knowledge Directory.
- If you installed the Oracle WebCenter Interaction Content Service for Documentum, import the migration packages located in *install_dir*/ptdctmcws/10.3.3/serverpackages:
  - DocumentumCS.pte
  - GlobalDocumentTypeMapDocumentum.pte
- If you installed the Oracle WebCenter Content Service for Oracle Universal Content Management, import the migration package located in *install_dir*/ptucmcws/10.3.3/serverpackages:
  - UCMCS_WS_RemoteServer.pte
- If you installed the Oracle WebCenter Interaction Identity Service for LDAP, import the migration package: located in *install_dir*/ptldapaws/10.3.3/serverpackages:
  - IdentityService-LDAP.pte
- If you installed the Oracle WebCenter JSR-168 Container, import the migration package located in *install_dir*/ptjsr168/10.3.3/serverpackages:
  - jsr-168-samples.pte

A

Completing Installation of the Tagging Engine

If you installed the Tagging Engine, perform the following tasks to complete the installation:

- Section A.1, "Seeding the ALUI Security Database with Tagging Engine Data"
- Section A.2, "Configuring the Tag Me Portlet"

A.1 Seeding the ALUI Security Database with Tagging Engine Data

This section describes how to trigger the Tagging Engine to seed the ALUI Security database with Tagging Engine delivered capabilities and default roles.

To seed the database:

1. Log in to the portal as a portal administrator.
2. Click **Administration**.
3. From the **Select Utility** menu, choose **Tagging Engine Administration**.

   Accessing the Tagging Engine Administration page will automatically seed the ALUI Security database

A.2 Configuring the Tag Me Portlet

This section describes how to configure the Tag Me portlet to work with the Tagging Engine.

To configure the Tag Me portlet:

1. Log in to the portal as a portal administrator.
2. Click **Administration**.
3. Open the **Portal Resources** folder, expand the **Web Services** section, then open the **Tag Me Web Service**.
4. On the left, click the **HTTP Configuration**.
5. Under Gateway URL Prefixes, replace the Tagging Engine remote server location with the correct URL (for example, `http://TaggingEngine/`.
6. Click **Finish**.
7. Open the Configuration Manager.
8. Confirm that Tagging Engine Integration is enabled.

Click **Portal Service**, then **Service Settings**, then **Tagging Engine Integration Settings**. Confirm that **enabled** is selected.

A.3 Troubleshooting

This section provides information on troubleshooting the installation and configuration process. It includes the following topics:

- Overview of Tagging Engine Logs
- When to Use the Logging Utilities

A.3.1 Overview of Tagging Engine Logs

This section provides the descriptions and locations of logs that you can use to troubleshoot the Tagging Engine installation and configuration. Individual log files are generated for each day's activity. The logs are stored in *install_dir*/installlogs.

Table A–1 Tagging Engine Installation Logs

Log	Description
pathways_deployment.log	Provides activity and error details for the installation of the main Tagging Engine UI files
searchservice_deployment.log	Provides activity and error details for the installation of the files required for integrating the Tagging Engine with the Oracle WebCenter Interaction search

A.3.2 When to Use the Logging Utilities

When the Tagging Engine portlets or the Tagging Engine Administration UI display either an error or the Tagging Engine diagnostic checks, the Tagging Engine or one or more of its required services may not be configured correctly. Use the Logging Utilities to help identify the specific issue by enabling the Tagging Engine and the required services as message senders within Logging Spy.

For more information about the Logging Utilities, see the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Interaction*.

B

Completing Installation of Oracle WebCenter Interaction Content Service for Documentum

If you installed Oracle WebCenter Interaction Content Service for Documentum, perform the following tasks to complete the installation:

B.1 Verifying Installation

Complete the steps on the Content Service for Documentum Installation Verification page. This page is located on your Oracle WebCenter Interaction Content Service for Documentum host computer, at http://*RemoteServer*:*port*/ptdctmcws/web/install/index.html.

B.2 Creating a Content Source

Create a content source to define the area of Documentum from which you want to import content. To create a content source, perform the following steps in the Oracle WebCenter Interaction Content Service for Documentum folder in the portal's Administrative Object Directory:

1. Log in to the portal as an administrator.
2. Click **Administration**.
3. Open the Oracle WebCenter Interaction Content Service for Documentum folder.
4. From the **Create Object** menu, select **Content Source - Remote**.
5. In the Choose Web Service dialog box, choose the **Oracle WebCenter Interaction Content Service for Documentum** Web service.
6. Configure the content source as described in the online help.

Stay logged in to the portal with the Oracle WebCenter Interaction Content Service for Documentum folder open for the next procedure.

B.3 Creating a Content Crawler

Create a content crawler to import content from the content source. To create a content crawler, perform the following steps in the Oracle WebCenter Interaction Content Service for Documentum folder of the portal's Administrative Object Directory:

1. From the **Create Object** menu, select **Content Crawler - Remote**.
2. In the Choose Content Source dialog box, choose the content source that you created in the previous procedure.
3. On the Main Settings page of the Content Crawler Editor, select **Import security with each document**. Configure the rest of the content crawler as described in the online help.

Stay logged in to the portal with the Oracle WebCenter Interaction Content Service for Documentum folder open for the next procedure.

B.4 Creating a Job

To import content, you must associate the content crawler with a job and run the job. To create and run a job, perform the following steps in the Oracle WebCenter Interaction Content Service for Documentum folder of the portal's Administrative Object Directory:

1. From the **Create Object** menu, select **Job**.
2. Click **Add Operation**.
3. Choose the content crawler that you created in the previous procedure.
4. Choose the scheduling values for the job and click **Finish**.
5. Name the job and click **OK**.
6. When you are finished creating the job, ensure that the Oracle WebCenter Interaction Content Service for Documentum folder is associated with an automation service. For assistance, see the online help under **Select Utilities**, then **Automation Service**.

B.5 Configuring Security for Document Discovery

Portal users discover documents by browsing the Knowledge Directory and using portal search tools. In the portal, you manage document discovery with access control lists (ACLs) that are associated with portal directories.

If you want Documentum users to be able to browse records for crawled Documentum records in the portal with a similar level of privilege they experience in the Documentum environment, you map the configuration for Documentum user privileges to the portal ACL Read privilege and ensure that their credentials are used for document *access*.

Note: You manage document *discovery* (display a record) as described in the following procedure. You manage document *access* (open a file) with click-through security, described in Section B.6, "Configuring Security for Document Access."

To configure security settings for the Oracle WebCenter Interaction Content Service for Documentum:

1. Deploy an authentication source (for example, LDAP) to manage Documentum users. For details, refer to Documentum documentation.
2. Create a remote authentication source in the portal to import the Documentum users. For details, refer to the portal's online help or the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Interaction*.
3. Configure the Global ACL Sync Map to associate the Documentum domain name with the authentication source:
   a. Log in to the portal as an administrator.
   b. Click **Administration**.
   c. From the **Select Utility** menu, select **Global ACL Sync Map**.
   d. Click **Add Mapping** and choose the authentication source you created in step 2.
   e. In the Domain Name column, click the edit icon and type the domain name of the Documentum users, usually the Lotus Domino Server name.
   f. Click **Finish**.
4. Set the `accessLevelMapping` setting in config.xml as follows.

Table B–1 accessLevelMapping Settings

Setting	Description
<accessLevelMapping>2</accessLevelMapping>	This is the default value and recommended value. This value enables portal document discovery for Documentum users with at least Browse access (Documentum Level 2 privilege).
<accessLevelMapping>3</accessLevelMapping>	This value restricts portal document discovery to Documentum users that have at least Read access (Documentum Level 3 privilege).

5. If you modify config.xml, you must restart the Web application server to initialize changes.

> **Note:** If you modified the accessLevelMapping, you must rerun crawl jobs with Refresh ACLs selected on the Advanced Settings page of the Crawler Editor to realize the changes.

Stay logged in to the portal for the next procedure.

B.6 Configuring Security for Document Access

To enable portal users to open files imported into the portal, you configure *click-through security*. The following table describes click-through security methods.

Table B–2 Click-Through Security Methods

Click-Through Security Method	Description and Procedure
User Preferences	User Preferences is the default click-through security method for Oracle WebCenter Interaction Content Service for Documentum. The User Preferences method uses stored values for the Documentum user to enable access to the Documentum file. To implement the User Preferences method, in the Oracle WebCenter Interaction Content Service for Documentum config.xml file (located by default in C:\Oracle\Middleware\wci\ptdctmcws\10.3.3\settings\config), set `clickthroughAuthType` as follows: `<clickthroughAuthType>1</clickthroughAuthType>` When users click through to a Documentum file for the first time, they are prompted for their Documentum credentials. The portal stores the credentials as user preferences, so the user does not have to enter them again. Users can modify the values of these credentials by clicking **My Account**, then **Oracle WebCenter Interaction Content Service for Documentum**.

Table B–2 (Cont.) Click-Through Security Methods

Basic Authentication	Basic Authentication is one of two SSO click-through security methods you can implement for Oracle WebCenter Interaction Content Service for Documentum. It uses the authentication information for the user portal session to enable access to the Oracle WebCenter Interaction Content Service for Documentum file. The portal user name must match the Documentum user name; so the portal and Documentum users must be synchronized from a common source, such as LDAP. **Note:** If you deploy this method, users must log in to the portal with both their user name and password. They cannot choose the Remember My Password option To enable Basic Authentication click-through: Disable User Preference click-through in the portal: **1.** In the portal's Administrative Object Directory, open the Oracle WebCenter Interaction Content Service for Documentum folder. **2.** Expand the Web Service section and click the **Oracle WebCenter Interaction Content Service for Documentum** Web service. **3.** On the left, under Edit Object Settings, click **Advanced URL Settings**. **4.** Remove the entry from the **User Configuration URL** box. **5.** On the left, under Edit Object Settings, click **Preferences**. **6.** Delete all User Preferences and click **Finish**. Stay logged in to the portal with the Oracle WebCenter Interaction Content Service for Documentum folder open for the next procedure. Enable Basic Authentication in the portal: **1.** In the portal PTConfig.xml file, set the `CaptureBasicAuthenticationForPortlets` parameter to **1**. **2.** In the Oracle WebCenter Interaction Content Service for Documentum folder of the portal's Administrative Object Directory, click the **Oracle WebCenter Interaction Content Service for Documentum** Web service. **3.** On the left, under Edit Object Settings, click **Authentication Settings**. **4.** Select **User's Basic Authentication Information**. **5.** Restart the portal application server. Enable Basic Authentication click-through on the Oracle WebCenter Interaction Content Service for Documentum host computer: **1.** In the Oracle WebCenter Interaction Content Service for Documentum config.xml file (located by default in C:\Oracle\Middleware\wci\ptdctmcws\10.3.3\settings\config), set `clickthroughAuthType` as follows: `<clickthroughAuthType>2</clickthroughAuthType>`

Table B–2 (Cont.) Click-Through Security Methods

Trusted Authentication	Trusted Authentication is one of two SSO click-through security methods you can implement for Oracle WebCenter Interaction Content Service for Documentum. It uses the authentication information from an SSO partner to enable access to the Documentum file. The portal user name must match the Documentum user name; so the portal and Documentum users must be synchronized from a common source, such as LDAP.
	
	To enable Trusted Authentication click-through:
	
	Disable User Preference click-through in the portal:
	
	1. In the portal's Administrative Object Directory, open the Oracle WebCenter Interaction Content Service for Documentum folder.
	
	2. Expand the Web Service section and click the **Oracle WebCenter Interaction Content Service for Documentum** Web service.
	
	3. On the left, under Edit Object Settings, click **Advanced URL Settings**.
	
	4. Remove the entry from the **User Configuration URL** box.
	
	5. On the left, under Edit Object Settings, click **Preferences**.
	
	6. Delete all User Preferences and click **Finish**.
	
	Stay logged in to the portal with the Oracle WebCenter Interaction Content Service for Documentum folder open for the next procedure.
	
	Enable Trusted Authentication click-through on the Oracle WebCenter Interaction Content Service for Documentum host computer:
	
	1. In the Oracle WebCenter Interaction Content Service for Documentum config.xml file (located by default in C:\Oracle\Middleware\wci\ptdctmcws\10.3.3\settings\config), set `clickthroughAuthType` as follows:
	
	`<clickthroughAuthType>3</clickthroughAuthType>`
	
	2. In config.xml file, specify the following parameters for the SSO partner:
	
	`<trustedUserName></trustedUserName>`
	`<trustedPassword></trustedPassword>`
	`<trustedDomain></trustedDomain>`
	
	Note: The value for the <trustedPassword> parameter must be encrypted. Use the **Encrypt Password** link located at: http://*RemoteServer:port*/ptdctmcws/web/install/index.html

Table B–2 (Cont.) Click-Through Security Methods

Admin Preference/Content Source Credential	If you prefer, you can set all click-through requests to use the credentials configured in the content source to retrieve documents upon click-through. This is referred to as the Super User click-through method. To enable Super User click-through: Disable User Preference click-through in the portal: 1. In the portal's Administrative Object Directory, open the Oracle WebCenter Interaction Content Service for Documentum folder. 2. Expand the Web Service section and click the **Oracle WebCenter Interaction Content Service for Documentum** Web service. 3. On the left, under Edit Object Settings, click **Advanced URL Settings**. 4. Remove the entry from the **User Configuration URL** box. 5. On the left, under Edit Object Settings, click **Preferences**. 6. Delete all User Preferences and click **Finish**. Stay logged in to the portal with the Oracle WebCenter Interaction Content Service for Documentum folder open for the next procedure. Enable content source credential click-through on the Oracle WebCenter Interaction Content Service for Documentum host computer: 1. In the Oracle WebCenter Interaction Content Service for Documentum config.xml file (located by default in C:\Oracle\Middleware\wci\ptdctmcws\10.3.3\settings\config), set `clickthroughAuthType` as follows: `<clickthroughAuthType>4</clickthroughAuthType>`

B.7 Setting the Preferred Document Rendition

The Documentum server stores *renditions* of documents (versions of documents in various formats). By default, Oracle WebCenter Interaction Content Service for Documentum returns the native version of the document. To set a preference to always retrieve PDF, Word, or text renditions, modify the <preferredRenditionFormat> element in config.xml (located by default in C:\Oracle\Middleware\wci\ptdctmcws\10.3.3\settings\config) as follows.

Table B–3 Possible Preferred Rendition Format Element Values

Value	Definition
default	This is the default and returns the document in its native format.
pdf	This specifies that the document be returned in PDF format, if available.
msw8	This specifies that the document be returned in Microsoft Word format, if available.
crtext	This specifies that the document be returned in text format, if available.

B.8 Advanced Configuration: Tuning Documentum Server

The instructions in this section provide additional steps for configuring the Documentum Server to work with the Oracle WebCenter Interaction Content Service for Documentum. This includes configuration changes on the computer that hosts the Documentum client and on the Documentum Server. We strongly recommend tuning Documentum to work with the Oracle WebCenter Interaction Content Service for Documentum. A typical production environment would have all of the recommended settings in place.

Note: For instructions on editing the dmcl.ini and server.ini files, refer to the *Documentum eContent Server Administrator's Guide*.

B.8.1 Modifying the dmcl.ini File on the Oracle WebCenter Interaction Content Service for Documentum Host

On all computers that host the Oracle WebCenter Interaction Content Service for Documentum, you can increase the `max_session_count` variable in the dmcl.ini file to allow for additional concurrent sessions. By default, the `max_session_count` is set to 10, meaning there can be 10 concurrent sessions to Documentum.

- The number of Documentum sessions depends on the number of content crawlers you expect to run concurrently, as well as the number of users you expect to click through links concurrently. We recommend you set the `max_session_count` parameter accordingly. You can increase this setting later if you find that you run out of sessions or want to increase the number of content crawlers running simultaneously.
- A session is started for each user with a unique user name/password that tries to click through to a Documentum document in the portal. The `max_session_count` must accommodate the estimated number of click through users to be handled concurrently.

B.8.2 Modifying the server.ini File on the Documentum Server

On the Documentum Server computer, you can change the settings in the server.ini file to allow for additional concurrent sessions.

- The `concurrent_sessions` variable controls the number of connections the Documentum server can handle concurrently. This parameter should accommodate for the sum of all the `max_session_count` values in your environment.

If you plan to use the Oracle WebCenter Interaction Content Service for Documentum with several different docbases, you must modify the server.ini for each docbase. When making these configuration changes, consider the following:

- As with any configuration changes, consider any hardware limitations.
- The configuration settings depend on both existing and projected Documentum usage.

B.9 Troubleshooting

This section provides reference information for troubleshooting problems you might encounter when you use the Oracle WebCenter Interaction Content Service for Documentum. It includes the following topics:

- Reviewing Log Files
- Modifying Configuration Files
- Diagnosing Unexpected Results

B.9.1 Reviewing Log Files

If you encounter problems with crawl jobs, you can review the job logs provided through the portal's Automation Service Utility. For details, refer to the portal's online

help or to the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Interaction*.

If you encounter problems with the Oracle WebCenter Interaction Content Service for Documentum, you can use Logging Spy to analyze portal communication.

The Oracle WebCenter Interaction Content Service for Documentum also logs communication on the Oracle WebCenter Interaction Content Service for Documentum host computer. To analyze logs specific to the Oracle WebCenter Interaction Content Service for Documentum processes, review the logs in *install_dir*/ptdctmcws/10.3.3/settings/logs.

B.9.2 Modifying Configuration Files

If you encounter error messages or logs that indicate misconfiguration in the Oracle WebCenter Interaction Content Service for Documentum config.xml file, you can modify the config.xml file to correct syntax or mismatched values.

The following table describes the syntax and values for config.xml configuration parameters.

Table B–4 Configuration Parameters

Configuration (sample value in bold)	Value Description
baseURL	The URL for the Oracle WebCenter Interaction Content Service for Documentum application on the Oracle WebCenter Interaction Content Service for Documentum host computer. When you configure Oracle WebCenter Interaction applications, always specify the fully qualified domain name for hosts to avoid host and domain name resolution mismatches.

Table B–4 (Cont.) Configuration Parameters

Configuration (sample value in bold)	Value Description
<clickthroughAuthType>**1**</clickthroughAuthType> <trustedUserName></trustedUserName> <trustedPassword></trustedPassword> <trustedDomain></trustedDomain>	The clickthroughAuth type parameter determines what type of authentication to use during click-through. The following values are valid: ■ 1 = User Preferences ■ 2 = Basic Authentication ■ 3 = Trusted Authentication ■ 4 = Admin Preferences We recommend you set the accessLevelMapping value to 3 (read) if the clickThroughAuthType is either 4 or 5. See Section B.5, "Configuring Security for Document Discovery," for details on accessLevelMapping. For Trusted authentication (option #3), credentials must be supplied below. The password must be encrypted. Follow the instructions on http://*RemoteServer*/ptdctmcws/web/install/index.html to generate an encrypted password.
<accessLevelMapping>**2**</accessLevelMapping>	The accessLevelMapping maps the Documentum access level setting to the portal's access privilege setting. Documentum users who have an access level setting that is equal to or higher than the value configured here will receive Read access in the portal. The default setting is 2 which means that Documentum users with Browse access or higher will receive Read access in the portal. Browse users will not, however, be able to click through and read the file contents because the Oracle WebCenter Interaction Content Service for Documentum verifies their credentials upon click-through and will not return the document unless they have Read access in Documentum. This is how the portal mimics the Documentum Browse-level security. An important dependency of this functionality is that userCredentialClickThrough must be set to true (see note above regarding setting this parameter to 3 if userCredentialClickThrough is set to false). Valid values for this parameter are: ■ 2 = Browse ■ 3 = Read
<preferredRenditionFormat>**default**</preferredRenditionFormat>	Set the preferredRenditionFormat to the desired format for the document to be returned during click-through. The portal supports the following formats: ■ default (or blank): The document's native format ■ pdf: Acrobat PDF ■ msw8: Microsoft Word 97/2000 ■ crtext: Text (Windows) The setting is "preferred" because the Oracle WebCenter Interaction Content Service for Documentum will return the native format for documents if pdf/msw8/crtext is not available. This option only applies if userCredentialClickThrough is set to true.

B.9.3 Diagnosing Unexpected Results

The following table summarizes cases in which users encountered unexpected results with the Oracle WebCenter Interaction Content Service for Documentum. You can use this table as a reference for particular issues you might encounter or as a guide for troubleshooting any similar problems you might encounter.

Table B–5 Troubleshooting

Symptom	Solution
HTTP 500 Error on Clickthrough Users have reported that the URL property in a document's Properties page is clickable, but the link returns an error. The URL property is unique as it is clickable in the Document Properties page (accessed by clicking **Properties** for a document crawled into the portal). This is potentially confusing to users because the value is technical and clicking it results in an HTTP 500 error.	To avoid potential confusion, map the URL property in a content type to an Override Value, such as a space, which will prevent the technical URL from appearing in the Properties page.
Crawl fails with [DM_API_E_NO_SESSION] error: "There are no more available sessions."	Increase the sessions in server.ini and dmcl.ini. For details, see Section B.8, "Advanced Configuration: Tuning Documentum Server.".
Port conflict, port in use, BindException	Port numbers for HTTP and HTTPS are configured in *install_dir*/ptdctmcws/10.3.3/settings/config/application.conf. Edit the http and https settings in application.conf to set the value to an available port. The service must be restarted to pick up changes made in the configuration file. Note that changes to a service port number require corresponding changes to any Web service or remote server settings that may reference that port number.
Memory consumption, Out of Memory Errors	The maximum amount of memory, in megabytes, that the service JVM will be allowed to use is controlled by the wrapper.java.maxmemory property, configured in the file *install_dir*/ptdctmcws/10.3.3/settings/config/wrapper.conf. For example, the following line shows a maximum memory setting of 1 GB: `wrapper.java.maxmemory=1024` The setting corresponds directly to the -Xmx parameter used by the java executable. The default value of this setting in the config file will be adequate for most configurations. For large production configurations, especially those in which the service is installed on a dedicated host computer, this value should be set as high as possible (for example, 1024 or 1536) but should always remain below the amount of physical RAM on the host computer.

C

Completing Installation of Oracle WebCenter Content Service for Oracle Universal Content Management

If you installed Oracle WebCenter Content Service for Oracle Universal Content Management, perform the following tasks to complete the installation:

C.1 Verifying Installation

Complete the steps on the Content Service for UCM Installation Verification page. This page is located on your Oracle WebCenter Content Service for Oracle Universal Content Management host computer, at http://*RemoteServer*:*port*/ptucmcws/web/install/index.html.

C.2 Creating a Content Source

Create a content source to define the area of Oracle Universal Content Management from which you want to import content. To create a content source, perform the following steps in the Oracle WebCenter Content Service for UCM folder in the portal's Administrative Object Directory:

1. Log in to the portal as an administrator.
2. Click **Administration**.
3. Open the Oracle WebCenter Content Service for UCM folder.
4. From the **Create Object** menu, select **Content Source - Remote**.
5. In the Choose Web Service dialog box, choose the **Oracle WebCenter Content Service for UCM** Web service.
6. Configure the content source as described in the online help.

Stay logged in to the portal with the Oracle WebCenter Content Service for UCM folder open for the next procedure.

C.3 Creating a Content Crawler

Create a content crawler to import content from the content source. To create a content crawler, perform the following steps in the Oracle WebCenter Content Service for UCM folder of the portal's Administrative Object Directory:

1. From the **Create Object** menu, select **Content Crawler - Remote**.
2. In the Choose Content Source dialog box, choose the content source that you created in the previous procedure.
3. On the Main Settings page of the Content Crawler Editor, select **Import security with each document**. Configure the rest of the content crawler as described in the online help.

Stay logged in to the portal with the Oracle WebCenter Content Service for UCM folder open for the next procedure.

C.4 Creating a Job

To import content, you must associate the content crawler with a job and run the job. To create and run a job, perform the following steps in the Oracle WebCenter Content Service for UCM folder of the portal's Administrative Object Directory:

1. From the **Create Object** menu, select **Job**.
2. Click **Add Operation**.
3. Choose the content crawler that you created in the previous procedure.
4. Choose the scheduling values for the job and click **Finish**.
5. Name the job and click **OK**.
6. When you are finished creating the job, ensure that the Oracle WebCenter Content Service for UCM folder is associated with an automation service. For assistance, see the online help under **Select Utilities**, then **Automation Service**.

C.5 Configuring Security for Document Discovery

Portal users discover documents by browsing the Knowledge Directory and using portal search tools. In the portal, you manage document discovery with access control lists (ACLs) that are associated with portal directories.

If you want Oracle Universal Content Management users to be able to browse records for crawled Oracle Universal Content Management records in the portal with a similar level of privilege they experience in the Oracle Universal Content Management environment, you map the configuration for Oracle Universal Content Management user privileges to the portal ACL Read privilege and ensure that their credentials are used for document *access*.

Note: You manage document *discovery* (display a record) as described in the following procedure. You manage document *access* (open a file) with click-through security, described in Section C.6, "Configuring Security for Document Access."

To configure security settings for the Oracle WebCenter Content Service for Oracle Universal Content Management:

1. Deploy an authentication source (for example, LDAP) to manage Oracle Universal Content Management users. For details, refer to Oracle Universal Content Management documentation.
2. Create a remote authentication source in the portal to import the Oracle Universal Content Management users. For details, refer to the portal's online help or the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Interaction*.
3. Configure the Global ACL Sync Map to associate the Oracle Universal Content Management domain name with the authentication source:
   a. Log in to the portal as an administrator.
   b. Click **Administration**.
   c. From the **Select Utility** menu, select **Global ACL Sync Map**.
   d. Click **Add Mapping** and choose the authentication source you created in step 2.
   e. In the Domain Name column, click the edit icon and type the domain name of the Oracle Universal Content Management users, usually the Lotus Domino Server name.
   f. Click **Finish**.

Stay logged in to the portal for the next procedure.

C.6 Configuring Security for Document Access

To enable portal users to open files imported into the portal, you configure *click-through security*. The following table describes click-through security methods.

Table C–1 Click-Through Security Methods

Click-Through Security Method	Description and Procedure
User Preferences	User Preferences is the default click-through security method for Oracle WebCenter Content Service for Oracle Universal Content Management. The User Preferences method uses stored values for the Oracle Universal Content Management user to enable access to the Oracle Universal Content Management file. To implement the User Preferences method, in the Oracle WebCenter Content Service for Oracle Universal Content Management config.xml file (located by default in C:\Oracle\Middleware\wci\ptucmcws\10.3.3\settings\config), set `clickthroughAuthType` as follows: `<clickthroughAuthType>1</clickthroughAuthType>` When users click through to a Oracle Universal Content Management file for the first time, they are prompted for their Oracle Universal Content Management credentials. The portal stores the credentials as user preferences, so the user does not have to enter them again. Users can modify the values of these credentials by clicking **My Account**, then **Oracle WebCenter Content Service for UCM**.

Table C–1 (Cont.) Click-Through Security Methods

Basic Authentication	Basic Authentication is one of two SSO click-through security methods you can implement for Oracle WebCenter Content Service for Oracle Universal Content Management. It uses the authentication information for the user portal session to enable access to the Oracle WebCenter Content Service for Oracle Universal Content Management file. The portal user name must match the Oracle Universal Content Management user name; so the portal and Oracle Universal Content Management users must be synchronized from a common source, such as LDAP. **Note:** If you deploy this method, users must log in to the portal with both their user name and password. They cannot choose the Remember My Password option To enable Basic Authentication click-through: Disable User Preference click-through in the portal: **1.** In the portal's Administrative Object Directory, open the Oracle WebCenter Content Service for UCM folder. **2.** Expand the Web Service section and click the **Oracle WebCenter Content Service for UCM** Web service. **3.** On the left, under Edit Object Settings, click **Advanced URL Settings**. **4.** Remove the entry from the **User Configuration URL** box. **5.** On the left, under Edit Object Settings, click **Preferences**. **6.** Delete all User Preferences and click **Finish**. Stay logged in to the portal with the Oracle WebCenter Content Service for UCM folder open for the next procedure. Enable Basic Authentication in the portal: **1.** In the portal PTConfig.xml file, set the `CaptureBasicAuthenticationForPortlets` parameter to **1**. **2.** In the Oracle WebCenter Content Service for UCM folder of the portal's Administrative Object Directory, click the **Oracle WebCenter Content Service for UCM** Web service. **3.** On the left, under Edit Object Settings, click **Authentication Settings**. **4.** Select **User's Basic Authentication Information**. **5.** Restart the portal application server. Enable Basic Authentication click-through on the Oracle WebCenter Content Service for Oracle Universal Content Management host computer: **1.** In the Oracle WebCenter Content Service for Oracle Universal Content Management config.xml file (located by default in C:\Oracle\Middleware\wci\ptucmcws\10.3.3\settings\config), set `clickthroughAuthType` as follows: `<clickthroughAuthType>2</clickthroughAuthType>`

Table C–1 (Cont.) Click-Through Security Methods

Trusted Authentication	Trusted Authentication is one of two SSO click-through security methods you can implement for Oracle WebCenter Content Service for Oracle Universal Content Management. It uses the authentication information from an SSO partner to enable access to the Oracle Universal Content Management file. The portal user name must match the Oracle Universal Content Management user name; so the portal and Oracle Universal Content Management users must be synchronized from a common source, such as LDAP.
	
	To enable Trusted Authentication click-through:
	
	Disable User Preference click-through in the portal:
	
	1. In the portal's Administrative Object Directory, open the Oracle WebCenter Content Service for UCM folder.
	2. Expand the Web Service section and click the **Oracle WebCenter Content Service for UCM** Web service.
	3. On the left, under Edit Object Settings, click **Advanced URL Settings**.
	4. Remove the entry from the **User Configuration URL** box.
	5. On the left, under Edit Object Settings, click **Preferences**.
	6. Delete all User Preferences and click **Finish**.
	
	Stay logged in to the portal with the Oracle WebCenter Content Service for UCM folder open for the next procedure.
	
	Enable Trusted Authentication click-through on the Oracle WebCenter Content Service for Oracle Universal Content Management host computer:
	
	1. In the Oracle WebCenter Content Service for Oracle Universal Content Management config.xml file (located by default in C:\Oracle\Middleware\wci\ptucmcws\10.3.3\settings\config), set `clickthroughAuthType` as follows:
	`<clickthroughAuthType>3</clickthroughAuthType>`
	2. In config.xml file, specify the following parameters for the SSO partner:
	`<trustedUserName></trustedUserName>`
	`<trustedPassword></trustedPassword>`
	`<trustedDomain></trustedDomain>`
	
	Note: The value for the <trustedPassword> parameter must be encrypted. Use the **Encrypt Password** link located at: http://*RemoteServer*:*port*/ptdctmcws/web/install/index.html

Table C–1 (Cont.) Click-Through Security Methods

Admin Preference/Content Source Credential	If you prefer, you can set all click-through requests to use the credentials configured in the content source to retrieve documents upon click-through. This is referred to as the Super User click-through method. To enable Super User click-through: Disable User Preference click-through in the portal: 1. In the portal's Administrative Object Directory, open the Oracle WebCenter Content Service for UCM folder. 2. Expand the Web Service section and click the **Oracle WebCenter Content Service for UCM** Web service. 3. On the left, under Edit Object Settings, click **Advanced URL Settings**. 4. Remove the entry from the **User Configuration URL** box. 5. On the left, under Edit Object Settings, click **Preferences**. 6. Delete all User Preferences and click **Finish**. Stay logged in to the portal with the Oracle WebCenter Content Service for UCM folder open for the next procedure. Enable content source credential click-through on the Oracle WebCenter Content Service for Oracle Universal Content Management host computer: 1. In the Oracle WebCenter Content Service for Oracle Universal Content Management config.xml file (located by default in C:\Oracle\Middleware\wci\ptucmcws\10.3.3\settings\config), set `clickthroughAuthType` as follows: `<clickthroughAuthType>4</clickthroughAuthType>`

C.7 Troubleshooting

This section provides reference information for troubleshooting problems you might encounter when you use the Oracle WebCenter Content Service for Oracle Universal Content Management. It includes the following topics:

- Reviewing Log Files
- Modifying Configuration Files
- Diagnosing Unexpected Results

C.7.1 Reviewing Log Files

If you encounter problems with crawl jobs, you can review the job logs provided through the portal's Automation Service Utility. For details, refer to the portal's online help or to the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Interaction*.

If you encounter problems with the Oracle WebCenter Content Service for Oracle Universal Content Management, you can use Logging Spy to analyze portal communication.

The Oracle WebCenter Content Service for Oracle Universal Content Management also logs communication on the Oracle WebCenter Content Service for Oracle Universal Content Management host computer. To analyze logs specific to the Oracle WebCenter Content Service for Oracle Universal Content Management processes, review the logs in *install_dir*/ptucmcws/10.3.3/settings/logs.

C.7.2 Modifying Configuration Files

If you encounter error messages or logs that indicate misconfiguration in the Oracle WebCenter Content Service for Oracle Universal Content Management config.xml file, you can modify the config.xml file to correct syntax or mismatched values.

The following table describes the syntax and values for config.xml configuration parameters.

Table C–2 Configuration Parameters

Configuration (sample value in bold)	Value Description
baseURL	The URL for the Oracle WebCenter Content Service for Oracle Universal Content Management application on the Oracle WebCenter Content Service for Oracle Universal Content Management host computer. When you configure Oracle WebCenter Interaction applications, always specify the fully qualified domain name for hosts to avoid host and domain name resolution mismatches.

Table C–2 (Cont.) Configuration Parameters

Configuration (sample value in bold)	Value Description
<clickthroughAuthType>**1**</clickthroughAuthType> <trustedUserName></trustedUserName> <trustedPassword></trustedPassword> <trustedDomain></trustedDomain>	The clickthroughAuth type parameter determines what type of authentication to use during click-through. The following values are valid: ■ 1 = User Preferences ■ 2 = Basic Authentication ■ 3 = Trusted Authentication ■ 4 = Admin Preferences We recommend you set the accessLevelMapping value to 3 (read) if the clickThroughAuthType is either 4 or 5. See Section C.5, "Configuring Security for Document Discovery," for details on accessLevelMapping. For Trusted authentication (option #3), credentials must be supplied below. The password must be encrypted. Follow the instructions on http://*RemoteServer*/ptucmcws/web/install/index.html to generate an encrypted password.
<accessLevelMapping>**2**</accessLevelMapping>	The accessLevelMapping maps the Oracle Universal Content Management access level setting to the portal's access privilege setting. Oracle Universal Content Management users who have an access level setting that is equal to or higher than the value configured here will receive Read access in the portal. The default setting is 2 which means that Oracle Universal Content Management users with Browse access or higher will receive Read access in the portal. Browse users will not, however, be able to click through and read the file contents because the Oracle WebCenter Content Service for Oracle Universal Content Management verifies their credentials upon click-through and will not return the document unless they have Read access in Oracle Universal Content Management. This is how the portal mimics the Oracle Universal Content Management Browse-level security. An important dependency of this functionality is that userCredentialClickThrough must be set to true (see note above regarding setting this parameter to 3 if userCredentialClickThrough is set to false). Valid values for this parameter are: ■ 2 = Browse ■ 3 = Read
<preferredRenditionFormat>**default**</preferredRenditionFormat>	Set the preferredRenditionFormat to the desired format for the document to be returned during click-through. The portal supports the following formats: ■ default (or blank): The document's native format ■ pdf: Acrobat PDF ■ msw8: Microsoft Word 97/2000 ■ crtext: Text (Windows) The setting is “preferred” because the Oracle WebCenter Content Service for Oracle Universal Content Management will return the native format for documents if pdf/msw8/crtext is not available. This option only applies if userCredentialClickThrough is set to true.

C.7.3 Diagnosing Unexpected Results

The following table summarizes cases in which users encountered unexpected results with the Oracle WebCenter Content Service for Oracle Universal Content Management. You can use this table as a reference for particular issues you might encounter or as a guide for troubleshooting any similar problems you might encounter.

Table C–3 Troubleshooting

Symptom	Solution
HTTP 500 Error on Clickthrough Users have reported that the URL property in a document's Properties page is clickable, but the link returns an error. The URL property is unique as it is clickable in the Document Properties page (accessed by clicking **Properties** for a document crawled into the portal). This is potentially confusing to users because the value is technical and clicking it results in an HTTP 500 error.	To avoid potential confusion, map the URL property in a content type to an Override Value, such as a space, which will prevent the technical URL from appearing in the Properties page.
Port conflict, port in use, BindException	Port numbers for HTTP and HTTPS are configured in *install_dir*/ptdctmcws/10.3.3/settings/config/application.conf. Edit the http and https settings in application.conf to set the value to an available port. The service must be restarted to pick up changes made in the configuration file. Note that changes to a service port number require corresponding changes to any Web service or remote server settings that may reference that port number.
Memory consumption, Out of Memory Errors	The maximum amount of memory, in megabytes, that the service JVM will be allowed to use is controlled by the wrapper.java.maxmemory property, configured in the file *install_dir*/ucmcws/10.3.3/settings/config/wrapper.conf. For example, the following line shows a maximum memory setting of 1 GB: `wrapper.java.maxmemory=1024` The setting corresponds directly to the -Xmx parameter used by the java executable. The default value of this setting in the config file will be adequate for most configurations. For large production configurations, especially those in which the service is installed on a dedicated host computer, this value should be set as high as possible (for example, 1024 or 1536) but should always remain below the amount of physical RAM on the host computer.

D

Completing Installation of Oracle WebCenter Interaction Identity Service for LDAP

If you installed Oracle WebCenter Interaction Identity Service for LDAP, perform the following tasks to complete the installation:

- Verifying Installation
- Creating a Remote Authentication Source
- Creating a Remote Profile Source
- Creating a Job

This chapter also include the section Section D.5, "Advanced Configuration," which includes the following optional advanced procedures for LDAP configuration:

- Configuring Logging
- Configuring Application Server Session Settings
- Configuring LDAP Server Settings
- Using Oracle WebCenter Interaction Identity Service for LDAP over SSL

D.1 Verifying Installation

After you have deployed the Oracle WebCenter Interaction Identity Service for LDAP package, you can run a diagnostic utility to verify connectivity among deployment components.

To verify your deployment of the Oracle WebCenter Interaction Identity Service for LDAP package:

1. In a Web browser, open the URL for the remote server diagnostics utility, for example: http://*RemoteServer*:*port*/ldapws/install/index.html
2. Complete the steps as described in the utility summary page to verify the correct configuration of deployment components.

D.2 Creating a Remote Authentication Source

Create a remote authentication source to import users and groups from LDAP:

1. Log in to the portal as an administrator.
2. Click **Administration**.
3. Click the LDAP IDS folder.

4. From the **Create Object** menu, choose **Authentication Source - Remote**.
5. In the Choose Web Service dialog box, choose **LDAP IDS**.
6. Configure the authentication source as described in the online help.

Stay logged in to the portal with the LDAP IDS folder open for the next procedure.

D.3 Creating a Remote Profile Source

Create a remote profile source to import users' profile information from LDAP. To create a remove profile source, in the LDAP IDS folder of the portal's Administrative Object Directory:

1. From the **Create Object** menu, choose **Profile Source - Remote**.
2. In the Choose Web Service dialog box, choose **LDAP IDS**.
3. Configure the profile source as described in the online help.

D.4 Creating a Job

To import users, groups, or users' profile information, you must associate the authentication source or profile source with a job and run the job. To create and run a job, perform the following steps in the Oracle WebCenter Interaction Identity Service for LDAP folder of the portal's Administrative Object Directory:

1. From the **Create Object** menu, select **Job**.
2. Click **Add Operation**.
3. Choose the authentication source or profile source that you created.
4. Choose the scheduling values for the job and click **Finish**.
5. Name the job and click **OK**.
6. When you are finished creating the job, make sure the Oracle WebCenter Interaction Identity Service for LDAP folder is associated with an automation service. For assistance, see the online help under **Select Utilities**, then **Automation Service**.

D.5 Advanced Configuration

This section describes the following optional advanced procedures for LDAP configuration:

- Configuring Logging
- Configuring Application Server Session Settings
- Configuring LDAP Server Settings
- Using Oracle WebCenter Interaction Identity Service for LDAP over SSL

D.5.1 Configuring Logging

The ldapws.war file includes the log4j.properties file. The log4j.properties controls the logging settings for the application. You can open the log4j.properties file and edit it within the ldapws.war file.

There are two appenders defined:

- A1 is for the authentication source log
- A2 is for the profile source log

The default settings for the parameters in this file should be sufficient but there are several settings that you can change:

Table D–1 Logging Settings

Files	Function
Append	Determines whether writes to the log file are appended at the end of the file, or if the file is overwritten. This should be set to true.
MaxFileSize	Specifies the maximum size a log file can be before it is rolled over into a new file if the appender is a `RollingFileAppender`. If you choose to roll over based on the date, the `MaxFileSize` setting does not take effect.
MaxBackupIndex	Sets the number of rolled-over files that are saved. The number of roll-over files you set for the `MaxBackupIndex` value depends on how much disk space you choose to devote to log files.
DatePattern	Determines the basis on which files are rolled over if the appender is a `DailyRollingFileAppender`. YYY-mm means the file is rolled over once a month. YYYY-mm-dd means the file is rolled over ever day. YYYY-mm-dd-HH rolls over every hour and so forth.
RollingFileAppender	If several synchronization jobs are run once a day use the `RollingFileAppender` so that the individual log files do not grow excessively large.
DailyRollingFIleAppender	In changing the `DailyRollingFileAppender` from `RollingFileAppender`, the `MaxFileSize` setting is ignored. This enables you to set the type of appender to either rollover based on date or size. If you use a `DailyRollingFileAppender` then you must look at the average size of the log created by a single synchronization run to determine what the total disk space is. If synchronizations are run once a week, then setting `MaxBackupIndex` to 10 provides approximately two months of job histories.

D.5.2 Configuring Application Server Session Settings

Within the ldapws.war file there is a web.xml file that includes settings for the application session. You can open this file and edit it within the ldapws.war file.

During large synchronizations, the portal must create database objects for all the users and groups returned by the Oracle WebCenter Interaction Identity Service for LDAP. This might cause session timeouts between the calls to GetGroups, GetUsers, and GetMembers.

You can avoid this timeout error by increasing the session-timeout value in the session-config object of web.xml.

D.5.3 Configuring LDAP Server Settings

LDAP servers allow you to set the maximum return size of a query result as well as the time limit for a query. If the Oracle WebCenter Interaction Identity Service for LDAP log file ever indicates a SizeLimitExceeded or TimeLimitExceeded error it is most likely that you must adjust these values on the LDAP server. Different LDAP server administration consoles have these settings in different locations and you should contact your LDAP system administrator if you have questions about the location of the settings.

D.5.4 Using Oracle WebCenter Interaction Identity Service for LDAP over SSL

to use the Oracle WebCenter Interaction Identity Service for LDAP over SSL there are two connections you must secure. This section includes the following topics:

- Setting Up SSL Between the Portal and the Remote Server
- Setting Up SSL Between the Remote Server and the LDAP Server

D.5.4.1 Setting Up SSL Between the Portal and the Remote Server

to connect to the Oracle WebCenter Interaction Identity Service for LDAP from the portal over SSL, you must connect to the remote server on an SSL port and import its trusted certificate.

From a Web browser on the portal server navigate to: https://*remote_server*:*app_server_ssl_port*.

If the computer hosting the portal does not already have a certificate from the remote server it prompts you with a Security Alert. Choose to view the certificate and install it to the Trusted Root Certification Authorities store.

When running the installer for Oracle WebCenter Interaction Identity Service for LDAP, choose https protocol and enter the SSL port for the application server. In the portal, when you configure the remote server object, use https and the SSL port.

D.5.4.2 Setting Up SSL Between the Remote Server and the LDAP Server

To connect to the LDAP server over SSL, import the certificate for the LDAP server into the cacerts file in the jre of the application server.

1. From a Web browser on the remote server navigate to: https://*ldap_server*:*ldap_ssl_port*. You should be prompted with a Security Alert.
2. Choose to view the certificate and import it.
3. Click **Tools**, then **Internet Options**.
4. Select the **Content** tab and click **Certificates**.
5. Find the certificate for the LDAP server that you just imported and choose to export it as a DER encoded binary. Export it to the APP_SERVER_JAVA_HOME/jre/lib/security folder.
6. Use the java keytool to import this certificate to the cacerts file at APP_SERVER_JAVA_HOME/jre/lib/security.

   For instructions on using the keytool refer to the SunJava documentation.

   When you create the authentication source in the portal, enter 2 as the Security Mode. The standard SSL port is 636. If your LDAP server is using a different SSL port, enter this in the Alternate Port box.

E

Completing Installation of Oracle WebCenter JSR-168 Container

If you installed Oracle WebCenter JSR-168 Container, perform the following tasks to complete the installation:

- Section E.1, "Configure Remote Server"
- Section E.2, "Install the Oracle WebCenter JSR-168 Container Samples"

E.1 Configure Remote Server

Add the path to Oracle WebCenter JSR-168 Container PT_HOME:

1. Navigate to the directory referenced by PT_HOME and open **pthome.xml** in a text editor.
2. Add the following code within the pthome element (between `<pthome>` and `</pthome>`).

> **Note:** The `<path>` and `<configpath>` elements must reflect the fully qualified path to the ptjsr168 directories. slashes must be used regardless of operating system.

```
<product name="ptjsr168">
<install version="10.3.3">
<path>/oracle/middleware/wci/ptjsr168/10.3.3</path>
<configpath>/oracle/middleware/wci/ptjsr168/settings/config</configpath>
</install>
</product>
```

E.2 Install the Oracle WebCenter JSR-168 Container Samples

To install the Oracle WebCenter JSR-168 Container samples:

1. Deploy the ali168Samples.war file from the *install_dir*/ptjsr168/10.3.3/samples directory using the method appropriate for your application server.
2. Migrate the jsr-168.pte server package using the method appropriate for the version of Oracle WebCenter Interaction installed. For details on importing server packages, see the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Interaction*.

The Oracle WebCenter JSR-168 Container server package is *install_dir*/ptjsr168/10.3.3/serverpackages/jsr-168.pte.

After the resource package is imported, a JSR-168 folder will appear in portal administration that includes the JSR-168 Remote Server, two Web Services (RSSPortletWebService and JspPortletWebService), and two portlets (RSSPortlet and JspPortlet). These portlets do not require any configuration.

Note: Before placing the portlets on a page, edit the JSR-168 Remote Server object and change the Remote Server URL to the correct address of the host computer.

Note: The sample RSSportlet contains an admin preference page that enables you to save your proxy server settings. You must configure your application server to work with a proxy server setting. Follow the documentation for your application server to configure the proxy server setting.

F

Uninstalling Oracle WebCenter Interaction

This chapter describes how to uninstall Oracle WebCenter Interaction.

> **Note:** You must stop all Oracle WebCenter Interaction services before uninstalling Oracle WebCenter Interaction.

1. Start the uninstaller. Execute install_dir/uninstall/ptportal/10.3.3/uninstall WebCenter_Interaction.
2. On the Uninstall Oracle WebCenter Interaction page, click **Next**.
3. On the Uninstall Options page, choose whether you want to perform a complete uninstall of Oracle WebCenter Interaction or to uninstall specific features. Then click **Next**.
4. On the Uninstall Complete page, review any items that could not be removed.

Index