Oracle® Fusion Middleware

Upgrade Guide for Oracle WebCenter Interaction

10*g* Release 4 (10.3.3.0.0) for Windows

E14551-07

May 2013

Describes how to upgrade Oracle WebCenter Interaction for Windows.

ORACLE

Oracle Fusion Middleware Upgrade Guide for Oracle WebCenter Interaction, 10*g* Release 4 (10.3.3.0.0) for Windows

E14551-07

Primary Author: Sarah Bernau

Contents

Preface

This book describes how to upgrade from Oracle WebCenter Interaction 10.3 or 10.3.0.1 to Oracle WebCenter Interaction for Microsoft Windows 10*g* Release 4 (10.3.3.0.0). It is designed to be a quick reference for users with upgrade experience, while also providing detailed instructions for users upgrading for the first time.

> **Note:** You can upgrade only from versions 10.3 or 10.3.0.1. If you run an older version, you must first upgrade to 10.3 before following the instructions in this guide. For instructions on upgrading to 10.3, see documentation available in the Oracle WebCenter Interaction 10*g* Release 3 (10.3) documentation set.

Audience

This documentation is written for the user responsible for upgrading 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 upgrade.

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
  - Lotus Notes Content Service
  - Windows File Content Service
  - Exchange 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
  - Active Directory 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.

- .NET integration services
  - Console for SharePoint

    Oracle WebCenter Console for Microsoft SharePoint imports, indexes, and returns Microsoft Windows Sharepoint Services resources through Oracle WebCenter Interaction Search.

1.1.1 Upgrade Roadmap

This section provides an overview of the steps necessary to upgrade and redeploy 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, "Prerequisites."
2. Run the installer as described in Chapter 3, "Upgrading the Oracle WebCenter Interaction Components."
3. Upgrade the databases used by Oracle WebCenter Interaction as described in Chapter 4, "Upgrading and Creating Databases for Oracle WebCenter Interaction."
4. Perform post-installation tasks such as restarting the Oracle WebCenter Interaction services, running diagnostics scripts to verify your installation, and rebuilding your search indexes as described in Chapter 5, "Post-Installation Tasks."
5. Perform additional post-installation tasks for optional components as described in the following appendices:
   - 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 or Upgrade 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 Content Service for Lotus Notes, complete the tasks described in Appendix D, "Completing Installation or Upgrade of Oracle WebCenter Interaction Content Service for Lotus Notes."
   - If you installed the Oracle WebCenter Interaction Content Service for Microsoft Windows Files, complete the tasks described in Appendix E,

"Completing Installation of Oracle WebCenter Interaction Content Service for Windows Files."

- If you installed the Oracle WebCenter Interaction Content Service for Microsoft Exchange, complete the tasks described in Appendix F, "Completing Installation of Oracle WebCenter Interaction Content Service for Microsoft Exchange."
- If you installed the Oracle WebCenter Interaction Identity Service for LDAP, complete the tasks described in Appendix G, "Completing Installation or Upgrade of Oracle WebCenter Interaction Identity Service for LDAP."
- If you installed the Oracle WebCenter Interaction Identity Service for Microsoft Active Directory, complete the tasks described in Appendix H, "Completing Installation or Upgrade of Oracle WebCenter Interaction Identity Service for Microsoft Active Directory."

2

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 with the upgrade.

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

1. Ensure you are running Oracle WebCenter Interaction 10.3 or 10.3.0.1.

   You can upgrade only from versions 10.3 or 10.3.0.1. If you run an older version, you must first upgrade to 10.3 before following the instructions in this guide. For instructions on upgrading to 10.3, see documentation available in the Oracle WebCenter Interaction 10*g* Release 3 (10.3) documentation set.

2. 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.

3. Read the product release notes for information on compatibility issues, known problems, and workarounds that might affect how you proceed with your deployment.

4. Provision host computers for your deployment and install prerequisite software. For details, see Section 2.1, "Software Requirements."

   Note: If you are running Microsoft Internet Information Server (IIS) 7, you must install the IIS 6 Management Compatibility suite (this option is available when installing IIS 7.

5. Back up configuration.xml. The installer will merge new settings into this file, and might, in the process, overwrite customizations you have made.

6. Ensure that you have administrative access to the resources you must complete installation and configuration tasks. For details, see Section 2.2, "Administrative User Requirements."

7. If you are installing the .NET portal on a 32 bit system, you must enable the /3GB switch in the Boot Configuration Data (BCD) store (for Windows 2008) or in the boot.ini file (for Windows 2003) on the Oracle WebCenter Interaction host computer. For details, see Section 2.3, "Virtual Memory Requirements for .NET Portals."

8. If you are using Oracle Database in your deployment, set the Oracle environment variables. For details, see Section 2.4, "Setting Oracle Environment Variables."

9. If you are using Oracle WebLogic Server in your deployment, disable Basic Authentication. For details, see Section 2.5, "Preparing Oracle WebLogic Server for Oracle WebCenter Interaction."

10. If you are installing Oracle WebCenter Interaction Content Service for Documentum for the first time, you must first install the Documentum DFC Runtime Environment. For details, see Section 2.6, "Configuring the Documentum DFC Runtime Environment."

11. If you are upgrading Oracle WebCenter Interaction Content Service for Documentum:

    a. If you have customized the config.xml and dql.xml configuration files, copy these files to a temporary location outside of the installation target path so that they are not overwritten by the installer.

    b. Uninstall the previous version of Oracle WebCenter Interaction Content Service for Documentum.

    Caution: If Professional Consulting Services (PCS) has made specialized customizations to the Oracle WebCenter Interaction Content Service for Documentum, do not upgrade on your own. Your customizations might not be included in the new version. Contact PCS to perform the upgrade.

    ---

12. If you are upgrading Oracle WebCenter Interaction Content Service for Lotus Notes, uninstall the previous version of Oracle WebCenter Interaction Content Service for Lotus Notes.

13. If you are installing Oracle WebCenter Interaction Content Service for Windows Files for the first time, register your .NET extensions in Microsoft Internet Information Services. For details, see Section 2.7, "Configuring Microsoft Internet Information Services for Oracle WebCenter Interaction Content Service for Windows Files."

14. If you are upgrading Oracle WebCenter Interaction Content Service for Windows Files:

    a. If you have customized the config.xml file, copy the file to a temporary location outside of the installation target path so that it is not overwritten by the installer.

    b. Uninstall the previous version of Oracle WebCenter Interaction Content Service for Windows Files.

15. If you are installing Oracle WebCenter Interaction Content Service for Microsoft Exchange for the first time, install a supported version of the Microsoft Outlook or Microsoft Exchange client, and create and configure a Windows user for use with this service. For details, see Section 2.8, "Creating a Domain User for Oracle WebCenter Interaction Content Service for Microsoft Exchange."

16. If you are upgrading Oracle WebCenter Interaction Content Service for Microsoft Exchange, uninstall the previous version of Oracle WebCenter Interaction Content Service for Microsoft Exchange.

17. If you are upgrading Oracle WebCenter Interaction Identity Service for LDAP, uninstall the previous version of Oracle WebCenter Interaction Identity Service for LDAP.

18. If you are upgrading Oracle WebCenter Console for Microsoft SharePoint, uninstall the previous version of Oracle WebCenter Console for Microsoft SharePoint.
19. If you are upgrading Oracle WebCenter Interaction Identity Service for Microsoft Active Directory, uninstall the previous version of Oracle WebCenter Interaction Identity Service for Microsoft Active Directory.

2.1 Software Requirements

For the latest information on supported operating systems, application servers, databases, and browsers, see the Oracle WebCenter Interaction page at http://www.oracle.com/technetwork/middleware/webcenter-interaction/index.html, open the Oracle WebCenter Interaction 10*g* Release 4 Certification Matrix 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 Administrative User Requirements

This section describes the administrative user permissions required to install Oracle WebCenter Interaction components on Microsoft Windows.

Table 2–1 Administrative User Permissions

User	Permissions
Local Host Administrator Account	The installing user must have local administrative rights. You must log in to the host computer as the local administrator.
Valid NT User	The installer requests the domain, user name, and password for a valid NT user.
Portal Database and Portal Administrative User Accounts	To configure the required portal database and portal administrative objects, you must provide the user name and password for the appropriate administrative user accounts.

2.3 Virtual Memory Requirements for .NET Portals

If you run your portal on .NET, you must enable the /3GB switch in the Boot Configuration Data (BCD) store (for Windows 2008) or in the boot.ini file (for Windows 2003) on the Oracle WebCenter Interaction host computer. The /3GB switch configures the user mode virtual address space available to each process.

To enable the /3GB switch for Windows 2008:

1. Log in to the Oracle WebCenter Interaction host computer as a user with Administrator privileges.
2. Open an elevated command prompt.
3. Run the following command:

```
BCDEDIT.EXE /Set IncreaseUserVa 3072
```

4. Reboot the portal host computer.

Note: You must add the /3GB flag to the BCD store correctly; editing the BCD store incorrectly might negatively affect the stability of your portal computer. For this reason, we strongly advise that you refer to appropriate documentation at http://msdn.microsoft.com when performing this procedure. If you experience technical difficulties, contact Microsoft support.

To enable the /3GB switch for Windows 2003:

1. Open the boot.ini file, which is located in the C: directory.

   The boot.ini file is hidden and read-only, so you must configure Windows to make hidden files visible and enable write privileges on the boot.ini file.

2. In the boot.ini file, add a /3GB flag to the end of the `multi` line, which specifies the partition to boot. For example:

   ```
   multi(0)disk(0)rdisk(0)partition(2)\WINDOWS="Windows Server 2003, Standard"
   /3GB /fastdetect /NoExecute=OptOut
   ```

3. Reboot the portal host computer.

Note: You must add the /3GB flag to the boot.ini file correctly; editing this file incorrectly might negatively affect the stability of your portal computer. For this reason, we strongly advise that you refer to appropriate documentation at http://msdn.microsoft.com when performing this procedure. If you experience technical difficulties, contact Microsoft support.

2.4 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.	▪ C:\oracle
ORACLE_HOME	Must be set to the *home* directory of your Oracle installation.	▪ C:\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.

2.5 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. 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
```

2.6 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.3.1, "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
```

2.7 Configuring Microsoft Internet Information Services for Oracle WebCenter Interaction Content Service for Windows Files

If you are installing Oracle WebCenter Interaction Content Service for Windows Files, you must configure Microsoft Internet Information Services (IIS) to work with your installation.

2.7.1 Registering .NET Extensions in IIS

The Oracle WebCenter Interaction Content Service for Windows Files installer expects .NET extensions to be registered and allowed in IIS.

To register .NET extensions from the command line, run the following:

```
<.net_directory>\aspnet_regiis.exe -i
```

To allow ASP.NET extensions:

1. Open IIS Manager. In the **Start** menu, click **Programs**, then **Administrative Tools**, then **Internet Information Services Manager**.
2. In the left pane of the IIS Manager, expand the node for the Web server and click **Web Service Extensions**.
3. In the right pane, view a list of Web service extensions and the status (Prohibited or Allowed) for each. Right-click the extension name and select **Allow** to enable it.

2.8 Creating a Domain User for Oracle WebCenter Interaction Content Service for Microsoft Exchange

If you are installing Oracle WebCenter Interaction Content Service for Microsoft Exchange, create and configure a Microsoft Windows domain user for use with this service:

1. Create a Microsoft Windows domain user named ali-exchangecs-user and provision an account for this user on the Microsoft Exchange Server. This administrative user runs the crawl jobs, so you should create the account for this purpose only.
2. On the remote server host computer, log in as ali-exchangecs-user, open Microsoft Outlook and dismiss any initialization screens.
3. Configure Microsoft Outlook as the default mail client for ali-exchangecs-user, and select the option to save the password.
4. Using the Microsoft Windows security policy manager, add the ali-exchangecs-user to the **Act as part of the operating system** policy.

5. Make sure ali-exchangecs-user can access all the Microsoft Exchange folders you want to crawl.
6. To test connectivity between the Microsoft Outlook client and the Microsoft Exchange Server, send mail from ali-exchangecws-user to ali-exchangecs-user.

Note: Oracle WebCenter Interaction Content Service for Microsoft Exchange does not send or receive mail. This step is only a test.

3

Upgrading the Oracle WebCenter Interaction Components

This chapter describes how to run the installer to upgrade the Oracle WebCenter Interaction components.

Before completing these steps you must complete the tasks described in Chapter 2, "Prerequisites."

> **Note:** Oracle WebCenter Interaction requires Microsoft Visual Studio C++ 2005 SP1 Runtime Libraries. If you do not have these libraries, you are given the option to let the installer install the EN localized version of these libraries.

3.1 Before Running the Installer

You must complete the following steps before using the installer to upgrade the Oracle WebCenter Interaction components:

1. If you have multiple search nodes in a search cluster, purge the contents of your search cluster using the `cadmin` tool.

   > **Note:** All nodes in the cluster must be running to purge cluster contents.

   a. Log in to any of the computers hosting a cluster node.

   b. Change to the directory containing the cluster administration utility.

      The directory is *install_dir*\ptsearchserver\10.3.3\bin

   c. Execute `cadmin purge --remove`

2. Shut down your search node(s):

   install_dir`\ptsearchserver\10.3.3\bin\searchserverd.bat stop`

   > **Note:** This must be done on each computer that hosts a search node.

3. Shut down your application server.

3.2 Running the Installer

Perform the following steps to run the installer:

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

   The installer file is named WebCenterInteraction_10.3.3.0.0.exe.
4. Complete the 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: C:\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.
Web Application Environment: .NET or Java	Select **.NET (IIS)** or **Java**.
Select IIS Web Site	If you chose .NET IIS as your Web application environment, select **Use Default Web Site** if you want the component or components being installed deployed to port 80, the default HTTP port. Select **Use another Web site** if other applications are using port 80 and you do not want to share the port.
Specify IIS Web Site Information	If you chose to deploy the portal to a Web site other than the default Web site, enter the IIS Web site name and HTTP and HTTPS ports you want to use for accessing the portal. Example Web site name: `WCI` Example HTTP port: `8082` Example HTTPS port: `9092` **Note**: If the name you enter is not the name of an existing IIS Web site, a new Web site is created. If the Web site already exists, the secure and non-secure ports will be changed to the entries made in the installer.
Auto-Deployment to a Java Web Application Server	If you chose Java as your Web application environment, select a Web application server to which you want to auto-deploy the Portal. Select Manual to manually deploy the portal to a Web application server.

Wizard Page	Description
Specify WebLogic Deployment Information	If you chose WebLogic as your Web application server, enter the Oracle WebLogic Server home directory, domain home, host name, port, domain, server, administrator user and administrator user password. **Note**: Oracle WebLogic Server domain and server names are case-sensitive. If the letter casing you enter does not match the running Oracle WebLogic Server domain and server, auto-deployment fails. Click Help for further details on this installer wizard page.
Image Service: Auto-Deployment to Apache	If you chose to manually deploy your Web application server, select **Apache** to have the Image Service automatically deployed to Apache. Select **Manual** if you prefer to use a Web server other than Apache.
Apache Deployment Information	If you chose to auto-deploy the image service to Apache, enter the Apache configuration directory. Example directory: `C:\Program Files\Apache Group\Apache2\conf\` Enter the Apache Windows service name. Example name: `Apache2`
Image Service Compression on IIS	The **Enable Image Service HTTP Compression** checkbox is selected by default. Clear the checkbox if you do not want to use HTTP compression.
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: `C:\Program Files\Documentum\dctm.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.

Wizard Page	Description
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**.
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.

4

Upgrading and Creating Databases for Oracle WebCenter Interaction

This chapter describes how to upgrade the portal database and create the new database necessary for the Tagging Engine.

It includes the following sections:

- Section 4.1, "Upgrading the Portal Database"
- Section 4.2, "Running the Database Upgrade Tool"
- Section 4.3, "Creating and Configuring the Tagging Engine Database"
- Section 4.4, "Creating and Configuring the ALUI Security Database"

> **Note:** Perform the steps in the order presented. If you run the Database Upgrade Tool before running the upgrade scripts, you receive a password seed error when you run the scripts.

4.1 Upgrading the Portal Database

This section describes how to upgrade the portal database. It includes the following sections:

- Upgrading the Portal Database on Oracle Database for Microsoft Windows
- Upgrading the Portal Database on Microsoft SQL Server

4.1.1 Upgrading the Portal Database on Oracle Database for Microsoft Windows

This section describes how to upgrade the Oracle WebCenter Interaction portal database on Oracle Database for Microsoft Windows.

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 2.4, "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_nt9.2

   - 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_nt10

   - 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_nt11

3. Run the upgrade10.3.0to10.3.3_oracle.sql script to upgrade the database.
4. Start the Oracle Listener for the portal database.

4.1.2 Upgrading the Portal Database on Microsoft SQL Server

This section describes how to upgrade the Oracle WebCenter Interaction portal database on Microsoft SQL Server.

1. Log in to the portal database host computer as the sa user so that the tables are owned by dbo.
2. Run the upgrade10.3.0to10.3.3_mssql.sql script to upgrade the database. The script is located in *install_dir*\ptportal\10.3.3\sql\mssql.

4.2 Running the Database Upgrade Tool

Note: Run the Database Upgrade Tool only after running the upgrade scripts.

The command line Database Upgrade Tool is used to upgrade a portal database to 10.3.3 specifications. You must run the tool twice. The first time you run the Database

Upgrade Tool, it creates a text file to hold the data required by the upgrade tool. You edit the file (entering parameters such as the location of various files), then run the upgrade tool again to perform the upgrade.

> **Note:** Your system must be properly configured to run the portal in order to use this application, as it relies on your portal configuration to know how to connect to the database and complete the upgrade.

1. Run the Database Upgrade Tool from $PORTAL_HOME\bin\dbupgradetool.bat.

   If you have a .NET portal, a GUI upgrade utility will be launched. If you have a Java portal, a command line utility will be launched.

2. Provide the Admin user name and password in the fields in the GUI tool or as parameters in the command line utility:

   - Admin User Name - type the name of the Administrator user that you created when you installed your 10.3.0.1 portal (not another user in the Administrators group). The default name is "Administrator," but you may have changed the name for security purposes after installation.

     > **Note:** The Admin User Name is case sensitive.

   - Password - type the password for the Administrator user. If this user has an empty password, do not type anything.

   The upgrade tool creates the upgradedata.properties file in *install_dir*\settings\portal.

3. When prompted to edit the property settings (in the GUI tool) or the properties file (in the command line utility), you can skip this step. There is no new data required for this release.

4. Run the Database Upgrade Tool again to begin upgrading the database. The upgrade can run for a few seconds or a few hours, depending on the size of your database. If the Database Upgrade Tool encounters errors or data inconsistencies, it does not stop. Instead it logs the errors to the file specified in Step 3.

5. When the database upgrade completes, you are notified of the status. If the upgrade completed successfully (without errors), skip to Step 7.

   > **Note:** If PTGROUPMEMBERSHIP has a materialized view you may see an error regarding inability to drop a view. This can be ignored.

6. If there were errors, you should examine the log file, identify solutions, restore the database to its previous state, fix the problems, and re-run the Database Upgrade Tool.

   > **Note:** You must restore the database to its original 10.3.0.1 state before you re-run the Database Upgrade Tool. The Database Upgrade Tool may modify the database even if it fails. Therefore, even if the upgrade did not complete successfully, the database is at least partially upgraded to 10.3.3 specifications.

7. If you changed the database credentials, change them back to use the Oracle WebCenter Interaction database user.

4.3 Creating and Configuring the Tagging Engine Database

This section describes how to create and configure a database for the Tagging Engine. It includes the following sections:

- Creating and Configuring the Tagging Engine Database on Microsoft SQL Server
- Creating and Configuring the Tagging Engine Database on Oracle Database

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

4.3.1 Creating and Configuring the Tagging Engine Database on Microsoft SQL Server

To create the Tagging Engine database on Microsoft SQL Server:

1. Copy the scripts from *install_dir*\pathways\10.3.3\sql\mssql to the database host computer.
2. In SQL Server Management Studio, access the database engine's properties.
3. Configure the database engine to use **SQL Server and Windows Authentication mode**.
4. Restart the database engine.
5. Create the Tagging Engine database user, configuring the Tagging Engine database user to use **SQL Server Authentication**.
6. Create the Tagging Engine database.

   Configure the size of the Tagging Engine database. The growth of the database is directly correlated to the number of objects present in the system. Objects include such things as tags, user preferences, and saved searches. Estimate 10 MB of growth per 100,000 objects. For example, if the Tagging Engine database stores roughly 100,000 new objects per day, you should anticipate growth of 3.65 GB per year.
7. Change the default database for the Tagging Engine database user to the Tagging Engine database.
8. Grant the Tagging Engine database user the db_owner role for the Tagging Engine database.
9. As the Tagging Engine database user, run the create_pathways_schema.sql script on the Tagging Engine database.
10. Run the install_pathways_seeddata.sql script on the Tagging Engine database.

4.3.2 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\windows 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. It includes the following sections:

- Creating and Configuring the ALUI Security Database on Microsoft SQL Server
- Creating and Configuring the ALUI Security Database on Oracle Database

> **Note:** You do not need to 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 Microsoft SQL Server

This section describes how to create and configure the ALUI Security database on Microsoft SQL Server.

1. On the computer on which you installed the Tagging Engine, copy the scripts from *install_dir*\pathways\10.3.3\sql\mssql to the ALUI Security database host computer.

   These scripts include the script that you will use to configure the ALUI Security database.

2. In SQL Server Management Studio, access the database engine's properties.

3. Configure the database engine to use **SQL Server and Windows Authentication mode**.

4. Restart the database engine.

5. Create the ALUI Security database user:

   a. Create the ALUI Security database user.
   b. Configure the ALUI Security database user to use **SQL Server Authentication**.
   c. Set the ALUI Security database user password to the password you designated when you planned your deployment.
6. Create the ALUI Security database.
7. Change the default database for the ALUI Security database user to the ALUI Security database.
8. Grant the ALUI Security database user the db_owner role for the ALUI Security database.
9. Create the ALUI Security database schema. Specify the ALUI Security database user as the schema owner.
10. Grant the ALUI Security database user the sysadmin server role.
11. Connect to the ALUI Security database as the ALUI Security database user, using **SQL Server Authentication**.
12. Run the create_security_tables.sql script, located in the folder that you copied in step 1.

4.4.2 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\windows to the ALUI Security database's host computer.

   This directory contains the script that you will use to configure the ALUI Security database.
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

Post-Installation Tasks

This chapter describes the tasks you must complete after you install and start Oracle WebCenter Interaction, such as configuring the BaseURL, merging changes from your previous deployment, deploying the portal application and Image Service to your application server, and rebuilding your search indexes.

Perform the following steps:

1. Add the BaseURL parameter to portalconfig.xml.

   The BaseURL parameter is a new openconfig setting. During upgrade, your original portalconfig.xml file is preserved so as not to overwrite your changes. This means that new settings will not appear in your portalconfig.xml file, and you must add them manually.

   To add the BaseURL parameter, using a text editor, and add the following to the portal:CachedSettings section of the portalconfig.xml file (located in *install_dir*\settings\portal:

   ```
   <setting name="BaseURL">
         <value xsi:type="xsd:string">strBaseURL</value>
   </setting>
   ```

   Note: You might want to reference the portalconfig.xml file that is installed with new installations, which is located in *install_dir*\uninstall\ptportal\10.3.3\register\common-settings\noarch\settings\portal\.

2. Merge any changes you had in your configuration.xml file to the newly installed configuration.xml file.

3. Merge any changes you had in your adaptive layout files to the new adaptive layout files.

   During upgrade, the files in *install_dir*\ptimages\imageserver\plumtree\portal\private\pagelayouts are backed up to *install_dir*\backup\ptimages\imageserver\plumtree\portal\private\pagelayouts. You must merge any changes you made to those files into the new files.

4. If necessary, deploy the portal application to your application server.

   If you are installing Oracle WebCenter Interaction to a Java application server and the portal was not autodeployed, you must manually deploy the portal WAR or

EAR to your application server. The portal WAR and EAR are located in *install_dir*\ptportal\10.3.3\webapp\.

- If you are deploying to Oracle WebLogic Server or IBM WebSphere, deploy portal.ear.

5. If necessary, deploy the Image Service to your application server.

   If you are installing Oracle WebCenter Interaction to a Java application server and the portal was not autodeployed, you must manually deploy the Image Service to your application server. For details, see Section 5.1, "Deploying the Image Service."

6. Restart your portal and search services. For details, see Section 5.2, "Starting the Oracle WebCenter Interaction Services.".

   Caution: Do not start the automation server service.

7. Rebuild the portal search index. For details, see Section 5.4, "Rebuilding the Search Index."

8. Upgrade any other Oracle WebCenter products you previously installed using the associated 10.3.0.1 installers.

   For example, if you use identity services, content services, Oracle WebCenter Collaboration, Oracle WebCenter Analytics, or any other Oracle WebCenter products, you must also upgrade those products. For details, see the upgrade guides for the associated products.

9. If you are using Oracle WebCenter Collaboration or Oracle-BEA AquaLogic Interaction Publisher, rebuild the associated search indexes.

   To rebuild the indexes, access the administration utility for each product through your portal. For details, see the following administrator guides:

   - *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Collaboration*
   - *Administrator Guide for AquaLogic Interaction Publisher*

10. Start your automation server service. For details, see Section 5.2, "Starting the Oracle WebCenter Interaction Services."

11. Perform additional post-upgrade tasks for optional components as described in the following appendices:

    - If you installed the Tagging Engine, complete the tasks described in Appendix A, "Completing Installation of the Tagging Engine."
    - If you installed or upgraded the Oracle WebCenter Interaction Content Service for Documentum, complete the tasks described in Appendix B, "Completing Installation or Upgrade 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 or upgraded the Oracle WebCenter Interaction Content Service for Lotus Notes, complete the tasks described in Appendix D, "Completing Installation or Upgrade of Oracle WebCenter Interaction Content Service for Lotus Notes."

- If you installed the Oracle WebCenter Interaction Content Service for Microsoft Windows Files, complete the tasks described in Appendix E, "Completing Installation of Oracle WebCenter Interaction Content Service for Windows Files."

  Note: There are no post-install steps if you upgraded Oracle WebCenter Interaction Content Service for Windows Files.

- If you installed the Oracle WebCenter Interaction Content Service for Microsoft Exchange, complete the tasks described in Appendix F, "Completing Installation of Oracle WebCenter Interaction Content Service for Microsoft Exchange."

  Note: There are no post-install steps if you upgraded Oracle WebCenter Interaction Content Service for Microsoft Exchange.

- If you installed or upgraded the Oracle WebCenter Interaction Identity Service for LDAP, complete the tasks described in Appendix G, "Completing Installation or Upgrade of Oracle WebCenter Interaction Identity Service for LDAP."
- If you installed or upgraded the Oracle WebCenter Interaction Identity Service for Microsoft Active Directory, complete the tasks described in Appendix H, "Completing Installation or Upgrade of Oracle WebCenter Interaction Identity Service for Microsoft Active Directory."
- If you installed the Oracle WebCenter JSR-168 Container, complete the tasks described in Appendix I, "Completing Installation of Oracle WebCenter JSR-168 Container."

5.1 Deploying the Image Service

Note: This step is unnecessary if you selected .NET IIS during installation, or if you instructed the installer to autodeploy the Image Service to Apache.

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. Save httpd.conf and exit the text editor.
5. When Apache HTTP Server is restarted, http://webserver:8082/imageserver/ should point to *install_dir*\ptimages\imageserver.

5.2 Starting the Oracle WebCenter Interaction Services

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

1. Go to the Windows Services control panel.

   In the **Start** menu, click **Control Panel**, then **Administrative Tools**, then **Services**, or, at the command prompt, type `services.msc`.

2. Start Oracle WCI Search *host_name*.

   Note: It is important that third-party virus scanners do not attempt to scan the search service archives.

3. Start Oracle WCI Search Cluster Manager.
4. Start Oracle WCI API Service.
5. Start Oracle WCI LDAP Directory.
6. Start Oracle WCI Automation Service.

   Caution: Do not start the automation service until you have rebuilt the portal search index, and, if necessary the Oracle WebCenter Collaboration and Oracle-BEA AquaLogic Interaction Publisher, search indexes

7. Start Oracle WCI Notification Service.
8. Start Oracle WCI Document Repository Service.
9. Start Oracle WCI Logger Service.
10. Start Oracle WebCenter Configuration Manager Service.
11. Start Oracle WCI Content Upload Service.
12. Start Oracle WCI Tagging Service.

13. Start Oracle WCI Search Service.
14. Start Oracle WCI Remote Portlet Service.
15. Start Oracle WCI Content Service for Documentum.
16. Start Oracle WCI Content Service for UCM.
17. Start Oracle WCI Content Service for Microsoft Exchange.
18. Start Oracle WCI Identity Service for LDAP.

5.3 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 after upgrade.

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

Run the diagnostics script before starting your portal for the first time after upgrade. 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.bat

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

5.4 Rebuilding the Search Index

This section describes the proper procedure for rebuilding your Search index.

> **Note:** We do not recommend clicking **Run Once** from the administrative folder or selecting **Run Once** from the Job Editor. If you click **Run Once** from the administrative folder, the job log is not available in the Job Editor, which may inhibit troubleshooting if the rebuild fails. If you select **Run Once** from within the Job Editor, the **Search Update Agent** is not scheduled to run again in the future.

1. Log in to the portal as the administrator.
2. Click **Administration**.
3. From the **Select Utility** drop-down menu, select **Search Service Manager**.
4. Schedule the next search repair to occur either in the past or in the very near future.
5. Click **Finish**.
6. Navigate to the administrative folder that contains the search update agents that are registered with the Automation Service.
7. Schedule a search update agents to run in the past or in the very near future.

8. Click **Finish**.

The next search update agent that runs rebuilds the search index.

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 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 or Upgrade of Oracle WebCenter Interaction Content Service for Documentum

If you installed or upgraded Oracle WebCenter Interaction Content Service for Documentum, perform the tasks in this chapter to complete the installation or upgrade.

This chapter includes the following sections:

- Verifying Installation or Upgrade
- Completing Upgrade
- Completing a New Installation

This chapter also includes the section Section B.4, "Monitoring and Troubleshooting Your Deployment," which includes the following information about monitoring and troubleshooting your deployment:

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

B.1 Verifying Installation or Upgrade

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 Completing Upgrade

If you upgraded Oracle WebCenter Interaction Content Service for Documentum perform the following steps:

1. If you had customizations in your old dql.xml file, overwrite the newly installed file with your previous version.
2. If you had customizations in your old config.xml file, make a backup of the newly installed config.xml file, then merge the customizations from your old config.xml file into the new config.xml file.
3. Open each content source that uses the Oracle WebCenter Interaction Content Service for Documentum and re-submit the credentials.

B.3 Completing a New Installation

If you installed Oracle WebCenter Interaction Content Service for Documentum for the first time, perform the steps in the following sections:

1. Advanced Configuration: Tuning Documentum Server
2. Setting the Preferred Document Rendition
3. Configuring Security for Document Discovery
4. Configuring Security for Document Access
5. Creating a Content Source
6. Creating a Content Crawler
7. Creating a Job

B.3.1 Advanced Configuration: Tuning Documentum Server

If you installed Oracle WebCenter Interaction Content Service for Documentum for the first time, you must tune the 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.3.1.1 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.3.1.2 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, take into account any hardware limitations.
- The configuration settings depend on both existing and projected Documentum usage.

B.3.2 Setting the Preferred Document Rendition

If you installed Oracle WebCenter Interaction Content Service for Documentum for the first time, you must set 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–1 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.3.3 Configuring Security for Document Discovery

If you installed Oracle WebCenter Interaction Content Service for Documentum for the first time, you must configure 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 users to be able to browse files crawled into the portal from Documentum 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 make sure 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.3.4, "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 Documentum server name.
   f. Click **Finish**.
4. Set the `accessLevelMapping` setting in config.xml as follows.

Table B–2 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.3.4 Configuring Security for Document Access

If you installed Oracle WebCenter Interaction Content Service for Documentum for the first time, you must configure 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.

B.3.4.1 Configuring Document Access with 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.

Each user should perform the following steps to set user preferences for click-through:

1. Log in to the portal.
2. Click **My Account**.
3. Click **Oracle WebCenter Interaction Content Service for Documentum**.
4. Enter the client you would like to use on click-through and your Documentum user name and password.
5. Click **Submit**.

B.3.4.2 Configuring Document Access with 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:

1. Disable User Preference click-through in the portal:
   a. In the portal's Administrative Object Directory, open the Oracle WebCenter Interaction Content Service for Documentum folder.
   b. Expand the Web Service section and click the **Oracle WebCenter Interaction Content Service for Documentum** Web service.
   c. On the left, under Edit Object Settings, click **Advanced URL Settings**.
   d. Remove the entry from the **User Configuration URL** box.
   e. On the left, under Edit Object Settings, click **Preferences**.
   f. 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.
2. Enable Basic Authentication in the portal:
   a. In the *install_dir*\settings\portal\portalconfig.xml file, set the `CaptureBasicAuthenticationForPortlets` parameter to **1**.
   b. 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.
   c. On the left, under Edit Object Settings, click **Authentication Settings**.
   d. Select **User's Basic Authentication Information**.

e. Restart the portal application server.

3. Enable Basic Authentication click-through on the Oracle WebCenter Interaction Content Service for Documentum host computer. 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>
```

B.3.4.3 Configuring Document Access with 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:

1. Disable User Preference click-through in the portal:

   a. In the portal's Administrative Object Directory, open the Oracle WebCenter Interaction Content Service for Documentum folder.

   b. Expand the Web Service section and click the **Oracle WebCenter Interaction Content Service for Documentum** Web service.

   c. On the left, under Edit Object Settings, click **Advanced URL Settings**.

   d. Remove the entry from the **User Configuration URL** box.

   e. On the left, under Edit Object Settings, click **Preferences**.

   f. 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.

2. Enable Trusted Authentication click-through on the Oracle WebCenter Interaction Content Service for Documentum host computer:

   a. 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>
   ```

   b. 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 to get an encrypted value for your password.

B.3.4.4 Configuring Document Access with Administrative Preferences

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:

1. 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.
2. Enable content source credential click-through on the Oracle WebCenter Interaction Content Service for Documentum host computer. 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.3.5 Creating a Content Source

If you installed Oracle WebCenter Interaction Content Service for Documentum for the first time, 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.3.6 Creating a Content Crawler

If you installed Oracle WebCenter Interaction Content Service for Documentum for the first time, 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.3.7 Creating a Job

If you installed Oracle WebCenter Interaction Content Service for Documentum for the first time, 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, make sure 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.4 Monitoring and Troubleshooting Your Deployment

This section provides reference information for monitoring the health of your deployment and 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.4.1 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.4.2 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–3 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–3 (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.3.3, "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.4.3 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–4 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.3.1, "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:

1. Verifying Installation
2. Configuring Security for Document Discovery
3. Configuring Security for Document Access
4. Creating a Content Source
5. Creating a Content Crawler
6. Creating a Job

This chapter also includes the section Section C.7, "Monitoring and Troubleshooting Your Deployment," which includes the following information about monitoring and troubleshooting your deployment:

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

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 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 users to be able to browse files crawled into the portal from Oracle Universal Content Management 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 make sure 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.3, "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.3 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.4 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.5 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.6 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, make sure 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.7 Monitoring and Troubleshooting Your Deployment

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.2, "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 or Upgrade of Oracle WebCenter Interaction Content Service for Lotus Notes

If you installed or upgraded Oracle WebCenter Interaction Content Service for Lotus Notes, verify your installation or upgrade as described in Verifying Installation or Upgrade.

If you installed Oracle WebCenter Interaction Content Service for Lotus Notes for the first time, perform the following tasks to complete the installation:

1. Configuring Security for Document Discovery
2. Creating a Content Source
3. Creating a Content Crawler
4. Creating a Job
5. Configuring User Preferences for Document Access
6. Configuring Remote Server Logging

D.1 Verifying Installation or Upgrade

To verify a successful installation or upgrade:

1. Ensure the ASPNET user has full control privileges to the IBM Lotus Notes data directory.
2. Open the installation test page in the following location: http://*server_name*:*port*/NotesCWS/Servlets/InstallTest.aspx

   Run the procedures using a valid IBM Lotus Notes ID and password.

D.2 Configuring Security for Document Discovery

If you installed Oracle WebCenter Interaction Content Service for Lotus Notes for the first time, you must configure security settings for the Oracle WebCenter Interaction Content Service for Lotus Notes. 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 users to be able to browse files crawled into the portal from IBM Lotus Notes with a similar level of privilege they experience in the IBM Lotus Notes environment, you map the configuration for IBM Lotus Notes user privileges to the

portal ACL Read privilege and make sure their credentials are used for document *access*.

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

1. Deploy an authentication source (for example, LDAP) to manage IBM Lotus Notes users. For details, refer to IBM Lotus Notes documentation.
2. Create a remote authentication source in the portal to import the IBM Lotus Notes 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 IBM Lotus Notes 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 enter the domain name of the IBM Lotus Notes users, usually the Lotus Domino Server name.
   f. Click **Finish**.

Note: Oracle WebCenter Interaction Content Service for Lotus Notes only maps group level security rights from IBM Lotus Notes groups to portal groups. It does not map user level security rights.

You will configure additional security settings in the Content Crawler Editor as described in Section D.4, "Creating a Content Crawler."

Stay logged in to the portal for the next procedure.

D.3 Creating a Content Source

Create a content source to define the area of IBM Lotus Notes from which you want to import content. To create a content source, perform the following steps in the portal:

1. Open the Oracle WebCenter Interaction Content Service for Lotus Notes folder.
2. From the **Create Object** menu, select **Content Source - Remote**.
3. In the Choose Web Service dialog box, choose the **Oracle WebCenter Interaction Content Service for Lotus Notes** Web service.
4. Configure the content source as described in the online help.

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

D.4 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 Lotus Notes folder of the portal:

1. From the **Create Object** menu, select **Content Crawler - Remote**.
2. In the Choose Content Source dialog box, choose the content source 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 Lotus Notes folder open for the next procedure.

D.5 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 Lotus Notes folder of the portal:

1. From the **Create Object** menu, select **Job**.
2. Click **Add Operation** and choose the content crawler created in the previous procedure.
3. Configure the rest of the job as described in the online help.
4. When you are finished creating the job, make sure the Oracle WebCenter Interaction Content Service for Lotus Notes folder is associated with an Automation Service. For assistance, see the online help under **Select Utilities** > **Automation Service**.

D.6 Configuring User Preferences for Document Access

The portal can be configured to automatically pass the IBM Lotus Notes user credential information to the remote server when a user clicks a IBM Lotus Notes document. If the user preference is not configured, the user will have to log in to IBM Lotus Notes on every document click-through.

Each user should perform the following steps to set user preferences for click-through:

1. Log in to the portal.
2. Click **My Account**.
3. Click **Oracle WebCenter Interaction Content Service for Lotus Notes**.
4. Enter the client you would like to use on click-through and your IBM Lotus Notes user name and password.
5. Click **Submit**.

D.7 Configuring Remote Server Logging

Oracle WebCenter Interaction Content Service for Lotus Notes keeps a log of errors and other information on the remote server. If you must troubleshoot the Oracle WebCenter Interaction Content Service for Lotus Notes remote server or you are curious how your crawls are progressing, you might want to change the logging level to record more information.

To change the logging level and view the current log:

1. Log in to the portal as an administrator.

2. Click **Administration**.
3. From the **Select Utility** menu, select **Oracle WebCenter Interaction Content Service for Lotus Notes**.
4. Select the appropriate logging level or view the most recent log.

Note: If you want to view the log files directly, the default location on the remote server is: *install_dir*\ptnotescws\10.3.3\Webapp\NotesCWS\log

---

E

Completing Installation of Oracle WebCenter Interaction Content Service for Windows Files

If you installed Oracle WebCenter Interaction Content Service for Windows Files for the first time, perform the following tasks to complete the installation:

1. Setting Up Security Rights for Oracle WebCenter Interaction Content Service for Windows Files
2. Verifying the Security Library
3. Configuring Security for Document Discovery
4. Creating a Content Source
5. Creating a Content Crawler
6. Creating a Job
7. Advanced Configuration

Note: IIS must be running to complete the tasks in this chapter.

Note: There are no post-install steps if you upgraded Oracle WebCenter Interaction Content Service for Windows Files.

E.1 Setting Up Security Rights for Oracle WebCenter Interaction Content Service for Windows Files

Each content source you set up must impersonate an NT domain user to access your file system. You might want to create an NT user specifically for use with each content source you intend to create and then ensure that those users have write access to the directory where Oracle WebCenter Interaction Content Service for Windows Files is installed. Use the following steps if you must add a user.

1. From the **Start** menu, click **Settings**, then **Control Panel**, then **Administrative Tools**.
2. Double-click **Local Security Policy**.
3. Expand the Local Policies folder.
4. Click the User Rights Assignment folder.

5. Double-click **Log on as Service**.
6. In the Local Security Policy Setting dialog box, click **Add**.
7. In the Select Users or Groups dialog box, select the user and click Add.
8. Click **OK**, and then **OK** again.
9. Double-click **Log on as Batch Job** and repeat steps 6-8.
10. Reboot your computer after the user rights are added.

E.2 Verifying the Security Library

To verify that Oracle WebCenter Interaction security library is encrypting and decrypting passwords properly:

1. Go to the directory on the computer on which you installed Oracle WebCenter Interaction Content Service for Windows Files. The default installation location is: C:\Oracle\Middleware\wci\ptntcws\10.3.3.
2. Navigate to the bin\native directory, relative to the folder designated in the previous step.
3. Double-click the ptcryptotest.exe file. This file includes a test application used to test Oracle WebCenter Interaction encryption and decryption.
4. A console opens and prints the progress of encrypting and decrypting a password. If the test has finished successfully, the console displays `Success!` and asks the user to press ENTER to finish. Verify that `Success!` is displayed on the console, then press ENTER to close the test application.

E.3 Configuring Security for Document Discovery

You must configure security settings for the Oracle WebCenter Interaction Content Service for Windows Files. 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 users to be able to browse files crawled into the portal from Microsoft Windows with a similar level of privilege they experience in the Microsoft Windows environment, you map the configuration for Microsoft Windows user privileges to the portal ACL Read privilege and ensure that their credentials are used for document *access*.

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

1. Deploy an authentication source (for example, Active Directory) to manage Microsoft Windows users. For details, refer to Microsoft Windows documentation.
2. Create a remote authentication source in the portal to import the Microsoft Windows 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 Microsoft Windows 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 enter the domain name of the Microsoft Windows users.

f. Click **Finish**.

You will configure additional security settings in the Content Crawler Editor as described in Section E.5, "Creating a Content Crawler."

Stay logged in to the portal for the next procedure.

E.4 Creating a Content Source

Create a content source to define the area of Microsoft Windows from which you want to import content. To create a content source, perform the following steps in the portal:

1. Open the Oracle WebCenter Interaction Content Service for Windows Files folder.
2. From the **Create Object** menu, select **Content Source - Remote**.
3. In the Choose Web Service dialog box, choose the **Oracle WebCenter Interaction Content Service for Windows Files** Web service.
4. Configure the content source as described in the online help.

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

E.5 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 Windows Files folder of the portal:

1. From the **Create Object** menu, select **Content Crawler - Remote**.
2. In the Choose Content Source dialog box, choose the content source 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 Windows Files folder open for the next procedure.

E.6 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 Windows Files folder of the portal:

1. From the **Create Object** menu, select **Job**.
2. Click **Add Operation**.
3. Choose the content crawler 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 Windows Files folder is associated with an Automation Service. For assistance, see the online help under **Select Utilities**, then **Automation Service**.

E.7 Advanced Configuration

This chapter provides instructions for editing advanced settings in the configuration file.

There are several advanced configuration settings that can be set in the configuration file Web.config. The default location is on the Oracle WebCenter Interaction Content Service for Windows Files host computer is C:\Oracle\Middleware\wci\ptntcws\10.3.3\Webapp\ntcws.

> **Note:** Only the parameters listed below should be changed in the Web.config file. Do not change any of the other parameters in the file.

1. Open Web.config in a text editor.
2. Oracle WebCenter Interaction Content Service for Windows Files keeps a log of errors and other information on the remote server. If a problem occurs with Oracle WebCenter Interaction Content Service for Windows Files, you might be directed by customer support to change the logging level from the default level of ERROR to DEBUG. To do so, find the text `<level value="ERROR"/>` and change the value to DEBUG: `<level value="DEBUG"/>`.

   > **Note:** The default location of the log files on the remote server is: C:\oracle\middlware\wci\ptntcws\10.3.3\Webapp\settings\logs.

3. If you do not want to use basic authentication information passed in the Basic Authentication headers for Oracle WebCenter Interaction Content Service for Windows Files content sources, but would rather specify a particular NT domain user to impersonate, find the text `<identity impersonate="false"/>` and change the value to TRUE: `<identity impersonate="true"/>`.

   For more information on content source authentication, refer to the online help.

4. It is possible for crawl jobs that handle a very large number of documents to fail as a result of a session having timed out.

   When you run a crawl, there are two sessions that are created: one for crawling folders and one for crawling documents.The folder session remains inactive while the document session is used to crawl all the documents in the folder. If you are crawling a folder with a very large number of documents, the folder session might exceed the default IIS session timeout of 80 minutes. When the portal attempts to hit this session that has timed out, the job fails.

   If you encounter this problem, increase the IIS session timeout in Web.config and on the ntcws virtual directory in IIS. To increase the timeout value in Web.config, find the following text and increase the timeout value in the last line:

```
<sessionState cookieless="false"
mode="InProc"
sqlConnectionString="data source=127.0.0.1;user id=sa;password="
```

```
stateConnectionString="tcpip=127.0.0.1:42424"
timeout="80"/>
```

> **Note:** To avoid having a large timeout setting, we recommend that you modify your directory structure such that there are not folders that have a large number of documents in them.

5. Save the file and restart IIS for the changes to take effect.

F

Completing Installation of Oracle WebCenter Interaction Content Service for Microsoft Exchange

If you installed Oracle WebCenter Interaction Content Service for Microsoft Exchange for the first time, perform the following tasks to complete the installation:

1. Configuring Security for Document Discovery
2. Creating a Content Source
3. Creating a Content Crawler
4. Creating a Job

> **Note:** There are no post-install steps if you upgraded Oracle WebCenter Interaction Content Service for Microsoft Exchange.

F.1 Configuring Security for Document Discovery

You must configure security settings for the Oracle WebCenter Interaction Content Service for Microsoft Exchange. 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 users to be able to browse files crawled into the portal from Microsoft Exchange with a similar level of privilege they experience in the Microsoft Exchange environment, you map the configuration for Microsoft Exchange user privileges to the portal ACL Read privilege and ensure that their credentials are used for document *access*.

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

1. Grant the ali-exchangecs-user full control to the Oracle WebCenter Interaction installation directory (for example, C:\Oracle\Middleware\wci\).

> **Note:** The ali-exchangecs-user is the user you created before installation, as described in Section 2.8, "Creating a Domain User for Oracle WebCenter Interaction Content Service for Microsoft Exchange."

2. Deploy an authentication source (for example, LDAP) to manage Microsoft Exchange users. For details, refer to Microsoft Exchange documentation.
3. Create a remote authentication source in the portal to import the Microsoft Exchange users. For details, refer to the portal's online help or the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Interaction*.
4. Configure the Global ACL Sync Map to associate the Microsoft Exchange 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 enter the domain name of the Microsoft Exchange users.
   f. Click **Finish**.
5. Open the Oracle WebCenter Interaction Content Service for Microsoft Exchange folder.
6. Expand the Web Service section and click the **Oracle WebCenter Interaction Content Service for Microsoft Exchange** Web service.
7. On the left, under Edit Object Settings, click **Advanced Settings**.
8. Select **Supports importing security with each document**.
9. Click **Finish**.

You will configure additional security settings in the Content Crawler Editor as described in Section F.3, "Creating a Content Crawler."

Stay logged in to the portal for the next procedure.

F.2 Creating a Content Source

Create a content source to define the area of Microsoft Exchange from which you want to import content. To create a content source, perform the following steps in the portal's Administrative Object Directory:

1. Open the Oracle WebCenter Interaction Content Service for Microsoft Exchange folder.
2. From the **Create Object** menu, select **Content Source - Remote**.
3. In the Choose Web Service dialog box, choose the **Oracle WebCenter Interaction Content Service for Microsoft Exchange** Web service.
4. Configure the content source as described in the online help.

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

F.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 Microsoft Exchange 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 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 Microsoft Exchange folder open for the next procedure.

F.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 Microsoft Exchange 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 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 Microsoft Exchange folder is associated with an automation service. For assistance, see the online help under **Select Utilities** > **Automation Service**.

G

Completing Installation or Upgrade of Oracle WebCenter Interaction Identity Service for LDAP

If you installed or upgraded Oracle WebCenter Interaction Identity Service for LDAP, perform the tasks in this chapter to complete the installation or upgrade.

This chapter includes the following sections:

- Verifying Installation or Upgrade
- Completing Upgrade
- Completing a New Installation

This chapter also includes the section Section G.4, "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

G.1 Verifying Installation or Upgrade

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.

G.2 Completing Upgrade

If you upgraded Oracle WebCenter Interaction Identity Service for LDAP perform the following steps:

1. Copy any template files you may have created from *install_dir*\ptldapaws\10.3\settings\ldap\templates to *install_dir*\ptldapaws\10.3.3\settings\config\ldap\templates.
2. Import the 10.3 encryption key to your 10.3.3 installation:
   a. In a Web browser, open the remote server diagnostics utility, which can be found at: http://*remoteserver:port*/ldapws/install/index.html.
   b. Complete the steps as described in the utility summary page in the diagnostics utility.
   c. At the encryption key import step, click **Import** and browse to the LDAPKeyStore file that was created for your version 10.3 installation and select the key. The file can be found at: *JRE_HOME_FOR_YOUR_OLD_APP_SERVER*\lib\ext\LDAPKeyStore.
   d. In the portal, go to the remote server object for Oracle WebCenter Interaction Identity Service for LDAP and change the port number to the one you set when you installed version 10.3.3.
3. Compare the configuration.xml file you backed up before you upgraded to the new version to confirm that all LDAP settings were merged correctly.

G.3 Completing a New Installation

If you installed Oracle WebCenter Interaction Content Service for Documentum for the first time, perform the steps in the following sections:

1. Creating a Remote Authentication Source
2. Creating a Remote Profile Source
3. Creating a Job

G.3.1 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.

G.3.2 Creating a Remote Profile Source

Create a remote profile source to import users' profile information from LDAP. To create a remote 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.

G.3.3 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**.

G.4 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

G.4.1 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 G–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.

Table G–1 (Cont.) Logging Settings

Files	Function
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.

G.4.2 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 time-outs between the calls to GetGroups, GetUsers, and GetMembers.

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

G.4.3 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.

G.4.4 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

G.4.4.1 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.

G.4.4.2 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.

H

Completing Installation or Upgrade of Oracle WebCenter Interaction Identity Service for Microsoft Active Directory

If you installed or upgraded Oracle WebCenter Interaction Identity Service for Microsoft Active Directory, perform the tasks in this chapter to complete the installation or upgrade.

This chapter includes the following sections:

This chapter also includes the section Section H.4, "Advanced Configuration," which includes the following advanced configuration options for Oracle WebCenter Interaction Identity Service for Microsoft Active Directory:

H.1 Verifying Installation or Upgrade

Verify installation or upgrade by navigating to the installation verification log file. For example: *install_dir*\WebCenter_Interaction_Identity_Service_for_Active_Directory_InstallLog.log.

> **Note:** After you have imported the migration package into the portal, you can also run a diagnostic utility to verify connectivity among deployment components. To verify deployment, in a Web browser open the URL for the Remote Server diagnostic utility. For example: http://*RemoteServer*/adws/install/index.html

H.2 Completing Upgrade

If you upgraded Oracle WebCenter Interaction Identity Service for Microsoft Active Directory perform the following steps:

1. If you previously edited the **sessionstate timeout** value in web.config, you must edit it again in the newly installed web.config file. For more information, see Section H.4.1, "Editing the Web.config File."
2. For each Microsoft Active Directory authentication source you previously created in the portal, re-enter the authentication password. Each installation of Oracle WebCenter Interaction Identity Service for Microsoft Active Directory encrypts this password using a different key.

H.3 Completing a New Installation

If you installed Oracle WebCenter Interaction Identity Service for Microsoft Active Directory for the first time, perform the steps in the following sections:

1. IIS Virtual Directory Settings
2. Windows Installation Directory Settings
3. Create a Remote Authentication Source
4. Create a Remote Profile Source
5. Creating a Job

H.3.1 IIS Virtual Directory Settings

To edit virtual directory time-out and security settings:

1. Open Internet Information Services.
2. Expand the IIS hierarchy as necessary, right-click the adaws virtual directory, and select **Properties**.
3. In the Properties dialog box, click **Configuration**.
4. In the Application Configuration dialog box, click the **Options** tab. The ASP Script timeout can be left at the default of 90 seconds.

   The Session timeout should be set to the same value as the timeout value specified in the web.config file. See Section H.4.1, "Editing the Web.config File," for more information.

   For synchronizations of large user directories, a timeout between 120 and 240 minutes is recommended.
5. Return to the Properties dialog box and click the **Directory Security** tab to edit anonymous access and authentication control. The account used for anonymous access can be either a local or domain user, but in most circumstances the local user IUSR is recommended.
6. When you are done, close the Properties dialog box.

H.3.2 Windows Installation Directory Settings

The Windows installation directory settings are located in *install_dir*\ptadaws\10.3.3\webapp\adaws (for example, C:\Oracle\Middleware\wci\ptadaws\10.3.3\webapp\adaws).

The following security settings are the minimum requirements needed for Oracle WebCenter Interaction Identity Service for Microsoft Active Directory and logging to work correctly:

- The local NETWORK SERVICE user must have Full Control rights. Allow NETWORK SERVICE and the SYSTEM group Full Control rights on the folder.
- The account used for anonymous access, described in Section H.3.1, "IIS Virtual Directory Settings," must have **Read and Execute, List Folder Contents**, and **Read** rights on the folder. Whether this is a domain user or the local IUSR user, this account will be a member of the Authenticated Users group. Allow Authenticated Users these rights on the folder.
- Administrators will want to be able to view and modify the content of the folder, so allow the Administrators group Full Control rights on the folder.

H.3.3 Create a Remote Authentication Source

After importing the pte file, you must create an authentication source:

1. In the Administrative Object Directory, open the Active Directory folder.
2. In the **Create Object** menu, click **Authentication Source - Remote**.
3. In the Choose Web Service dialog box, select **Active Directory** (the Web service created during import), and click **OK**.
4. On the Remote Active Directory Agent Configuration page, fill out the information specific to your Active Directory server. For more information, refer to online help.
5. Create a job to run your authentication source:
   a. Open an administrative folder.
   b. In the **Create Object** menu, click **Job**.
   c. Complete the Job Editor. For more information, refer to online help.

H.3.4 Create a Remote Profile Source

After importing the pte file and creating a remote authentication source, you must create a remote profile source:

1. In the Administrative Object Directory, open the Active Directory folder.
2. In the **Create Object** menu, click **Profile Source - Remote**.
3. In the Choose Web Service dialog box, select **Active Directory (2)** (the Web service created during import), and click **OK**.
4. On the Remote Active Directory Configuration page, fill out the information specific to your Active Directory server. For more information, refer to online help.
5. Create a job to run your profile source:
   a. Open an administrative folder.
   b. In the **Create Object** menu, click **Job**.
   c. Complete the Job Editor. For more information, refer to online help.

H.3.5 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 Microsoft Active Directory 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 Microsoft Active Directory folder is associated with an automation service. For assistance, see the online help under **Select Utilities**, then **Automation Service**.

H.4 Advanced Configuration

This chapter describes the following advanced configuration options for Oracle WebCenter Interaction Identity Service for Microsoft Active Directory:

- Editing the Web.config File
- Active Directory Server Query Timeouts
- Active Directory Errors During GetMembers

H.4.1 Editing the Web.config File

There are several configurable settings in the Web.config file that help you avoid some common error cases and define logging parameters. If you want to edit the Web.config file, it can be found in the following location: *install_dir*\ptadaws\10.3.3\webapp\adaws (for example, C:\Oracle\Middleware\wci\ptadaws\10.3.3\webapp\adaws\Web.config).

H.4.1.1 Logging Settings

Within the Web.config file, locate the `log4net` section. The default settings for the parameters in this section should be sufficient in most cases, but there are several settings that you can change.

The log files created by log4net.dll are self-cleaning based on the following parameters:

- `MaximumFileSize` - Specifies the maximum size a log file can be before it is rolled over into a new file if RollingStyle is set to Size.
- `MaxSizeRollBackups` - Sets the number of rolled-over files that are saved.

Additional log4net- Settings are based on these parameters:

- `AppendToFile` - Determines whether writes to the log file will be appended to the end of the file, or if the file will be overwritten. This should be set to true.
- `RollingStyle` - Can be set to Size or Date.
- `StaticLogFileName` - When set to true means that the active file name will always be ADAWSLog.txt. Rollover files will be renamed with .1, .2, .3, and so on extensions. This should be set to true.

With the default settings, the most disk space that will ever be used by logging is 100MB.

The log level can be set to INFO, ERROR, or FATAL. The default setting of INFO provides information that describes when the Web service is called and what

parameters are provided, as well as logging any failures and their causes. The ERROR setting logs only failures. A setting of FATAL runs silently.

Even with the log level set to INFO, the logging for a single synchronization run never exceeds 10MB.

Note: The log4net.dll handles all log file creation and deletion. Deleting rollover files that were created by log4net while it is still running causes log4net to fail, and furthermore causes the Oracle WebCenter Interaction Identity Service for Microsoft Active Directory to fail. Because of this, rollover files should not be deleted manually. If they are, restart IIS to ensure that log4net continues to run properly. The rollover files can be viewed and copied without any adverse affect.

H.4.1.2 Logging Best Practices

When setting the logging practices, you should not delete or modify the rollover files. You should let log4net handle log file manipulation. The following three sections indicate the best settings for your environment.

H.4.1.3 Choosing An Appropriate Rolling Style

If several synchronization jobs are run a day, you may wish to set the `RollingStyle` to `Size`, so that the individual log files do not grow too large. If synchronization jobs are only run once a day or less, you may chose to set the `RollingStyle` to `Date`. The log files do not grow too large because they contain one run and the log for a single run never splits between two files (unless the job runs past midnight). If you choose to rollover based on `Date`, the `MaximumFileSize` setting does not take affect.

If synchronization jobs are run past midnight, using `Date` causes the log for a single synchronization job to be split into two files (due to the rollover at midnight). It is therefore recommended to use `Size` and to set the `MaximumFileSize` based upon the typical log size for a single run.

H.4.1.4 Recommendation for the Number of Rollover Files

The number of rollover files you set for the `MaxSizeRollBackups` value depends on how much disk space you choose to devote to log files. If `RollingStyle` is set to `Size` then it is easy to calculate the amount of space used. It is the `MaximumFileSize` you set multiplied by the `MaxSizeRollBackups` value. If you rollover based on `Date` 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 `MaxSizeRollBackups` to 10 provides approximately two months of job histories. If synchronizations are run on a daily basis then you may wish to increase the number of rollover files to keep a history that exceeds ten days.

H.4.1.5 Archiving Log Files

You may wish to keep a permanent archive of all the logs on another computer, or simply wish to keep a larger history than the one determined by the `MaxSizeRollBackups` setting. You can manually copy the files before the rollover limit is reached and they are overwritten. You could also set up a recurring task that copies files to another location. The frequency of this task is determined by the frequency of your synchronization runs, and your logging settings.

Note: Do not delete or move the rollover files without restarting IIS.

H.4.1.6 IIS Session Timeouts

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

This timeout error can be avoided by increasing the timeout value for the `sessionState` object. To avoid this large timeout from applying to both authentication calls and synchronization calls, create two directories for Oracle WebCenter Interaction Identity Service for Microsoft Active Directory. Make a copy of the directory and give it a different name.

In one of the files, set the timeout to a very large minute value for synchronization. In the other file, leave it at the default or decrease it to 5 minutes for authentication.

Create two virtual directories. One directory should point to the physical directory with the large timeout value. This directory is used for the synchronization URL. The other virtual directory points to the physical directory that contains the smaller timeout value. This virtual directory is used for the authentication URL.

For a complete discussion of IIS sessions, refer to the Release Notes.

Note: The timeout setting in the Web.config should match the session timeout for the virtual directory. See Section H.3.1, "IIS Virtual Directory Settings," for details on setting this timeout value.

H.4.2 Active Directory Server Query Timeouts

There is the potential for an Active Directory server timeout during synchronizations of especially large query bases or difficult query filters. A Microsoft DirectoryServices.dll bug causes this timeout to occur. The effect of this bug is that no exception is thrown, and instead a partial list is returned. Refer to the Release Notes for a full discussion of the consequences. The Microsoft (MS hotfix number Q833789) patch is included in the Oracle WebCenter Interaction Identity Service for Microsoft Active Directory release package.

Once the patch is installed, DirectoryServices.dll correctly passes on the timeout exception to the Web.config file.

At the top, in the `configSections`, you must uncomment the line with section name `= "system.directoryservices"`. This line also includes a `PublicKeyToken` value that must be set. This is the public key for your System.DirectoryServices.dll. To find this key, use the strong name tool `sn.exe -T system.directoryservices.dll`.

You must also uncomment the system.directoryservices section in the web.config file, and set `waitForPagedSearchData` to true. Remember that if you do this, Oracle WebCenter Interaction Identity Service for Microsoft Active Directory waits and blocks until all results are returned from the Active Directory server.

H.4.3 Active Directory Errors During GetMembers

Occasionally, Active Directory reports an error when it tries to get the members of a specific group. This error is a result of the server not having access to specific groups

from other domains, being temporarily unavailable, or a specific group having a bad membership attribute. Normally these Active Directory errors are caught and passed on by Oracle WebCenter Interaction Identity Service for Microsoft Active Directory. When the synchronization job encounters this error, it reports a failure and ends.

If you prefer that groups that cause an Active Directory error during `GetMembers` are simply skipped and allow the job to continue processing other groups, then set the `GetMembersActionOnError` key to Skip instead of Fail in the Web.config file.

Completing Installation of Oracle WebCenter JSR-168 Container

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

1. Disable Default Portlet Deployment on IBM AIX 6.1
2. Configure Remote Server
3. Install the Oracle WebCenter JSR-168 Container Samples

I.1 Disable Default Portlet Deployment on IBM AIX 6.1

If the JSR-168 portlets are deployed on IBM AIX 6.1 using WAS 7, disable the default portlet deployment:

1. Navigate to the Web application and open **web.xml** in a text editor.
2. Add the following setting to the web.xml file:

```
<context-param>

<param-name>com.ibm.websphere.portletcontainer.PortletDeploymentEnabled</param
-name>
   <param-value>false</param-value>
</context-param>
```

I.2 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">
<path>C:\oracle\middleware\wci\ptjsr168\10.3.3</path>
```

```
<configpath>C:\oracle\middleware\wci\ptjsr168\10.3.3\settings\config</configpat
h>
</install>
</product>
```

I.3 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.

J

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. Use Add/Remove Programs to remove Oracle 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