

## **Oracle® Fusion Middleware**

Installation Guide for Oracle WebCenter Interaction

10g Release 4 (10.3.3.0.0) for Windows

**E14549-06**

May 2013

Describes how to install Oracle WebCenter Interaction for Windows.

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

E14549-06

Copyright © 2011, 2013, Oracle and/or its affiliates. All rights reserved.

Primary Author: Sarah Bernau

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

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

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

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

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

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

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

---

---

# Contents

<b>Preface</b> .....	ix
Audience .....	ix
Documentation Accessibility .....	ix
Related Documents .....	ix
Conventions .....	x
<b>1 Oracle WebCenter Interaction Installer Overview</b>	
1.1 Oracle WebCenter Interaction Components .....	1-1
1.1.1 Installation Roadmap .....	1-4
<b>2 Installation Prerequisites</b>	
2.1 Software Requirements .....	2-2
2.2 Administrative User Requirements .....	2-2
2.3 Virtual Memory Requirements for .NET Portals .....	2-2
2.4 Setting Oracle Environment Variables .....	2-3
2.5 Preparing Oracle WebLogic Server for Oracle WebCenter Interaction .....	2-3
2.6 Preparing Microsoft Internet Information Services 7.0 for Oracle WebCenter Interaction .....	2-4
2.7 Configuring the Documentum DFC Runtime Environment .....	2-5
2.8 Configuring Microsoft Internet Information Services for Oracle WebCenter Interaction Content Service for Windows Files .....	2-5
2.8.1 Registering .NET Extensions in IIS .....	2-5
2.9 Creating a Domain User for Oracle WebCenter Interaction Content Service for Microsoft Exchange .....	2-6
<b>3 Installing Oracle WebCenter Interaction</b>	
3.1 Installing the Oracle WebCenter Interaction Components .....	3-1
3.2 Oracle WebCenter Interaction Installer Wizard Pages .....	3-2
3.3 Deploying the Image Service .....	3-4
<b>4 Creating and Configuring Databases for Oracle WebCenter Interaction</b>	
4.1 Creating and Configuring the Portal Database .....	4-1
4.1.1 Creating and Configuring the Portal Database on Oracle Database for Microsoft Windows .....	4-1
4.1.1.1 Creating the Portal Database on Oracle9i for Microsoft Windows .....	4-2

4.1.1.2	Creating the Portal Database on Oracle Database 10g or 11g for Microsoft Windows	4-3
4.1.1.3	Creating the Portal Tablespace on Oracle Database for Microsoft Windows	4-5
4.1.1.4	Creating the Portal Schema on Oracle Database for Microsoft Windows	4-5
4.1.2	Creating and Configuring the Portal Database on Microsoft SQL Server	4-6
4.1.2.1	Creating and Configuring the Portal Database on Microsoft SQL Server	4-6
4.1.2.2	Scripting the Portal Database on Microsoft SQL Server	4-6
4.2	Creating and Configuring the Notification Service Database	4-7
4.2.1	Creating an External Notification Database on Oracle Database	4-8
4.2.2	Creating an External Notification Database on Microsoft SQL Server	4-8
4.3	Creating and Configuring the Tagging Engine Database	4-9
4.3.1	Creating and Configuring the Tagging Engine Database on Microsoft SQL Server	4-9
4.3.2	Creating and Configuring the Tagging Engine Database on Oracle Database	4-9
4.4	Creating and Configuring the ALUI Security Database	4-10
4.4.1	Creating and Configuring the ALUI Security Database on Microsoft SQL Server	4-10
4.4.2	Creating and Configuring the ALUI Security Database on Oracle Database	4-11

## 5 Postinstallation Tasks

5.1	Starting the Oracle WebCenter Interaction Services	5-2
5.2	Running the Diagnostics Script	5-2
5.3	Starting the Portal	5-3
5.4	Importing Migration Packages	5-3

## A Completing Installation of the Tagging Engine

A.1	Seeding the ALUI Security Database with Tagging Engine Data	A-1
A.2	Configuring the Tag Me Portlet	A-1
A.3	Troubleshooting	A-2
A.3.1	Overview of Tagging Engine Logs	A-2
A.3.2	When to Use the Logging Utilities	A-2

## B Completing Installation of Oracle WebCenter Interaction Content Service for Documentum

B.1	Verifying Installation	B-1
B.2	Creating a Content Source	B-1
B.3	Creating a Content Crawler	B-2
B.4	Creating a Job	B-2
B.5	Configuring Security for Document Discovery	B-2
B.6	Configuring Security for Document Access	B-3
B.7	Setting the Preferred Document Rendition	B-8
B.8	Advanced Configuration: Tuning Documentum Server	B-8
B.8.1	Modifying the dmcl.ini File on the Oracle WebCenter Interaction Content Service for Documentum Host	B-9
B.8.2	Modifying the server.ini File on the Documentum Server	B-9
B.9	Troubleshooting	B-9
B.9.1	Reviewing Log Files	B-9
B.9.2	Modifying Configuration Files	B-10

B.9.3	Diagnosing Unexpected Results.....	B-13
-------	------------------------------------	------

## **C Completing Installation of Oracle WebCenter Content Service for Oracle Universal Content Management**

C.1	Verifying Installation.....	C-1
C.2	Creating a Content Source.....	C-1
C.3	Creating a Content Crawler.....	C-2
C.4	Creating a Job .....	C-2
C.5	Configuring Security for Document Discovery.....	C-2
C.6	Configuring Security for Document Access.....	C-3
C.7	Troubleshooting .....	C-8
C.7.1	Reviewing Log Files .....	C-8
C.7.2	Modifying Configuration Files .....	C-9
C.7.3	Diagnosing Unexpected Results.....	C-12

## **D Completing Installation of Oracle WebCenter Interaction Content Service for Lotus Notes**

D.1	Verifying Installation.....	D-1
D.2	Configuring Security .....	D-1
D.3	Creating a Content Source.....	D-2
D.4	Creating a Content Crawler.....	D-2
D.5	Creating a Job .....	D-2
D.6	Configuring User Preferences for Click-Through.....	D-3
D.7	Configuring Remote Server Logging.....	D-3

## **E Completing Installation of Oracle WebCenter Interaction Content Service for Windows Files**

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

## **F Completing Installation of Oracle WebCenter Interaction Content Service for Microsoft Exchange**

F.1	Configuring Security .....	F-1
F.2	Creating a Content Source.....	F-2
F.3	Creating a Content Crawler.....	F-2
F.4	Creating a Job .....	F-2

## **G Completing Installation of Oracle WebCenter Interaction Identity Service for LDAP**

G.1	Verifying Installation.....	G-1
G.2	Creating a Remote Authentication Source .....	G-1
G.3	Creating a Remote Profile Source .....	G-2
G.4	Creating a Job .....	G-2
G.5	Advanced Configuration .....	G-2
G.5.1	Configuring Logging.....	G-2
G.5.2	Configuring Application Server Session Settings .....	G-3
G.5.3	Configuring LDAP Server Settings .....	G-3
G.5.4	Using Oracle WebCenter Interaction Identity Service for LDAP over SSL .....	G-4
G.5.4.1	Setting Up SSL Between the Portal and the Remote Server .....	G-4
G.5.4.2	Setting Up SSL Between the Remote Server and the LDAP Server .....	G-4

## **H Completing Installation of Oracle WebCenter Interaction Identity Service for Microsoft Active Directory**

H.1	Verifying Installation.....	H-1
H.2	IIS Virtual Directory Settings .....	H-1
H.3	Windows Installation Directory Settings .....	H-2
H.4	Create a Remote Authentication Source.....	H-2
H.5	Create a Remote Profile Source.....	H-3
H.6	Creating a Job .....	H-3
H.7	Advanced Configuration .....	H-3
H.7.1	Editing the Web.config File .....	H-4
H.7.1.1	Logging Settings .....	H-4
H.7.1.2	Logging Best Practices .....	H-4
H.7.1.3	Choosing An Appropriate Rolling Style .....	H-5
H.7.1.4	Recommendation for the Number of Rollover Files .....	H-5
H.7.1.5	Archiving Log Files .....	H-5
H.7.1.6	IIS Session Timeouts.....	H-5
H.7.2	Active Directory Server Query Timeouts.....	H-6
H.7.3	Active Directory Errors During GetMembers .....	H-6

## **I Completing Installation of Oracle WebCenter JSR-168 Container**

I.1	Configure Remote Server.....	I-1
I.2	Install the Oracle WebCenter JSR-168 Container Samples .....	I-1

## **J Completing Installation of Oracle WebCenter Console for Microsoft SharePoint**

J.1	Verifying Installation.....	J-1
J.2	Creating a Content Source .....	J-1
J.3	Creating a Content Crawler.....	J-2
J.4	Creating a Job .....	J-3
J.4.1	Crawling RSS Site Feeds .....	J-4

## **K Uninstalling Oracle WebCenter Interaction**

### **Index**





---

---

# Preface

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

## Audience

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

## Documentation Accessibility

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

### Access to Oracle Support

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

## Related Documents

For more information, see the following documents in the Oracle WebCenter Interaction 10g 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:

<b>Convention</b>	<b>Meaning</b>
<b>boldface</b>	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	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.

---

---

# 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 Installation Roadmap

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

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





---

---

## Installation Prerequisites

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

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

1. Download the most up-to-date documentation from the Oracle Technology Network in the Oracle WebCenter Interaction 10g Release 4 (10.3.3.0.0) documentation set.
2. Read the product release notes for information on compatibility issues, known problems, and workarounds that might affect how you proceed with your deployment.
3. Provision host computers for your deployment and install prerequisite software. For details, see [Section 2.1, "Software Requirements."](#)

---

---

**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).

---

---

4. 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."](#)
5. 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."](#)
6. If you are using Oracle Database in your deployment, set the Oracle environment variables. For details, see [Section 2.4, "Setting Oracle Environment Variables."](#)
7. 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."](#)
8. If you are using Microsoft Internet Information Services 7.0 in your deployment, you must install the IIS 6.0 Management Compatibility Components. For details, see [Section 2.6, "Preparing Microsoft Internet Information Services 7.0 for Oracle WebCenter Interaction."](#)

9. If you are installing Oracle WebCenter Interaction Content Service for Documentum, you must first install the Documentum DFC Runtime Environment. For details, see [Section 2.7, "Configuring the Documentum DFC Runtime Environment."](#)
10. If you are installing Oracle WebCenter Interaction Content Service for Windows Files, register your .NET extensions in Microsoft Internet Information Services. For details, see [Section 2.8, "Configuring Microsoft Internet Information Services for Oracle WebCenter Interaction Content Service for Windows Files."](#)
11. If you are installing Oracle WebCenter Interaction Content Service for Microsoft Exchange, 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 2.9, "Creating a Domain User for Oracle WebCenter Interaction Content Service for Microsoft Exchange."](#)

## 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 10g 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 Oracle9i or Oracle Database 10g.

Environment Variable	Description	Example Values
ORACLE_BASE	Must be set to the <i>root</i> directory of your Oracle installation.	<ul style="list-style-type: none"> <li>■ C:\oracle</li> </ul>
ORACLE_HOME	Must be set to the <i>home</i> directory of your Oracle installation.	<ul style="list-style-type: none"> <li>■ C:\oracle\ora92</li> </ul>
ORACLE_SID	Must be set to the system ID (SID) of the portal database instance.	<ul style="list-style-type: none"> <li>■ (Oracle9i) PLUM</li> <li>■ (Oracle Database 11g) PLUM11</li> </ul> <p><b>Note:</b> 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.</p>

## 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 Preparing Microsoft Internet Information Services 7.0 for Oracle WebCenter Interaction

This section describes configuration of Microsoft Internet Information Services 7.0 required before the installation and deployment of Oracle WebCenter Interaction.

1. In the Start menu, click **All Programs**, then **Administrative Tools**, then **Server Manager**.
2. In the left pane of the Server Manager, expand the node for **Roles**, right-click **Web Server (IIS)**, then click **Add Role Services**.
3. In the Role Services list, select **IIS 6 Management Compatibility**.
4. Click **Next**.
5. Click **Install**.

## 2.7 Configuring the Documentum DFC Runtime Environment

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

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

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

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

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

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

## 2.8 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.

### 2.8.1 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.

## 2.9 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-exchangeecs-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-exchangeecs-user, open Microsoft Outlook and dismiss any initialization screens.
3. Configure Microsoft Outlook as the default mail client for ali-exchangeecs-user, and select the option to save the password.
4. Using the Microsoft Windows security policy manager, add the ali-exchangeecs-user to the **Act as part of the operating system** policy.
5. Ensure that the ali-exchangeecs-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-exchangeecs-user to ali-exchangeecs-user.

---

---

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

---

---

---

---

## Installing Oracle WebCenter Interaction

This chapter describes how to install the Oracle WebCenter Interaction components and how to deploy the portal application and Image Service to your application server.

### 3.1 Installing the Oracle WebCenter Interaction Components

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

---

---

**Notes:**

- If you install all the Oracle WebCenter Interaction components on one computer, the computer becomes overloaded and services will stop intermittently. To avoid this situation, install the components on two or more computers. For example, you might want to install the Administrative Portal Server, Automation Server, and API Service on one computer; Search on a second computer, and the remaining components on a third computer.
  - 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.
- 
- 

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.

For details, see [Section 3.2, "Oracle WebCenter Interaction Installer Wizard Pages"](#)

5. 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.
6. 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. The Image Service files are located in *install\_dir\ptimages\imageserver\*.

For instructions, see [Section 3.3, "Deploying the Image Service."](#)

## 3.2 Oracle WebCenter Interaction Installer Wizard Pages

This section describes the Oracle WebCenter Interaction installer wizard pages.

Wizard Page	Description
Introduction	This installer wizard page provides a brief description of the installer and describes how to run the installer in silent mode.
Installation Folder	Accept the default installation folder or select a different folder in which to install Oracle WebCenter Interaction. Default: C:\Oracle\Middleware\wci
Choose Components	Select either <b>Complete</b> or <b>Custom</b> . If you select <b>Complete</b> , a full set of <b>Oracle WebCenter Interaction</b> components is installed. If you select <b>Custom</b> , 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 <b>.NET (IIS)</b> or <b>Java</b> .
Select IIS Web Site	If you chose .NET IIS as your Web application environment, select <b>Use Default Web Site</b> if you want the component or components being installed deployed to port 80, the default HTTP port. Select <b>Use another Web site</b> 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 <b>Note:</b> 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	<p>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.</p> <p><b>Note:</b> 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.</p> <p>Click Help for further details on this installer wizard page.</p>
Image Service: Auto-Deployment to Apache	<p>If you chose to manually deploy your Web application server, select <b>Apache</b> to have the Image Service automatically deployed to Apache.</p> <p>Select <b>Manual</b> if you prefer to use a Web server other than Apache.</p>
Apache Deployment Information	<p>If you chose to auto-deploy the image service to Apache, enter the Apache configuration directory.</p> <p>Example directory: C:\Program Files\Apache Group\Apache2\conf\</p> <p>Enter the Apache Windows service name.</p> <p>Example name: Apache2</p>
Image Service Compression on IIS	<p>The <b>Enable Image Service HTTP Compression</b> check box is selected by default. Clear the check box if you do not want to use HTTP compression.</p>
Standalone or Cluster	<p>Select whether you would like to install a <b>Single Standalone Search Node</b> or add a <b>Search Cluster Node</b>. 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.</p>
Adding New Search Node	<p>Enter the name and port number of the new search node.</p> <p>The search node is installed into <i>install_dir\ptsearchserver\10.3.3</i>.</p>
Search Cluster Files	<p>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.</p> <p>Example: <i>install_dir\ptsearchserver\10.3.3\cluster</i></p>
Content Service for Documentum - Application Port	<p>Choose whether to use a secure protocol (https) for the Oracle WebCenter Interaction Content Service for Documentum or a standard protocol (http).</p> <p>Specify your port number. The default port is 11951. Make sure to enter the SSL port number if using https.</p>
Documentum Client Library	<p>Enter the path to your Documentum client library.</p> <p>Example: C:\Program Files\Documentum\dtm.jar</p>
Fully Qualified Domain Name	<p>Enter the fully qualified domain name for the computer hosting Oracle WebCenter Interaction Content Service for Windows Files.</p>
Identity Service for LDAP - Application Port	<p>Choose whether to use a secure protocol (https) for the Oracle WebCenter Interaction Identity Service for LDAP or a standard protocol (http).</p> <p>Specify your port number. The default port is 11950. Make sure to enter the SSL port number if using https.</p>

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 <b>Install</b> .
Launch Configuration Manager	<p>Launch the Configuration Manager.</p> <p>The Configuration Manager is located at:  <code>https://host:port</code></p> <p>Where <i>host</i> is the host you are installing on and <i>port</i> is the port you specified.</p> <p>Log in to the Configuration Manager using the user name <code>administrator</code> and the password you specified on the Configuration Manager – Port and Password page.</p> <p>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 <i>Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Interaction</i>.</p> <p>When you have completed all Configuration Manager tasks, return to the installer.</p>
Application Settings Confirmation	Choose whether you have completed configuration of your application settings or want to complete configuration later.
Install Complete	<p>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 <b>Done</b>.</p> <p><b>Note:</b> 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.</p>

### 3.3 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\.



---

---

# Creating and Configuring Databases for Oracle WebCenter Interaction

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

It includes the following sections:

- [Creating and Configuring the Portal Database](#)
- [Creating and Configuring the Notification Service Database](#)
- [Creating and Configuring the Tagging Engine Database](#)

## 4.1 Creating and Configuring the Portal Database

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

- [Creating and Configuring the Portal Database on Oracle Database for Microsoft Windows](#)
- [Creating and Configuring the Portal Database on Microsoft SQL Server](#)

### 4.1.1 Creating and Configuring the Portal Database on Oracle Database for Microsoft Windows

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

---

---

**Notes:**

- When running Oracle WebCenter Interaction with Oracle Database 11g 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 11g 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 Oracle9i, the Oracle WebCenter Interaction installer creates the SQL scripts in the following directories:
 

```
install_dir\ptportal\10.3.3\sql\oracle_nt9.2
install_dir\aluidirectory\1.1\sql\oracle
```
  - For Oracle Database 10g, the Oracle WebCenter Interaction installer creates the SQL scripts in the following directories:
 

```
install_dir\ptportal\10.3.3\sql\oracle_nt10
install_dir\aluidirectory\1.1\sql\oracle
```
  - For Oracle Database 11g, the Oracle WebCenter Interaction installer creates the SQL scripts in the following directories:
 

```
install_dir\ptportal\10.3.3\sql\oracle_nt11
install_dir\aluidirectory\1.1\sql\oracle
```
3. Configure the portal database, tablespace, and user.
  - If you are creating a new Oracle9i database for the Oracle WebCenter Interaction schema, see [Section 4.1.1.1, "Creating the Portal Database on Oracle9i for Microsoft Windows."](#)
  - If you are creating a new Oracle Database 10g or 11g for the Oracle WebCenter Interaction schema, see [Section 4.1.1.2, "Creating the Portal Database on Oracle Database 10g or 11g for Microsoft Windows."](#)
  - If you are creating the Oracle WebCenter Interaction tablespace and schema within an existing Oracle database, see [Section 4.1.1.3, "Creating the Portal Tablespace on Oracle Database for Microsoft Windows."](#)
4. Create the portal schema and initialize the portal database.
 

For details, see [Section 4.1.1.4, "Creating the Portal Schema on Oracle Database for Microsoft Windows."](#)
5. Start the Oracle Listener for the portal database.

#### 4.1.1.1 Creating the Portal Database on Oracle9i for Microsoft Windows

This section describes how to create and configure the portal database, tablespace, and user on Oracle9i.

---



---

**Note:** These steps create a new, dedicated portal database. If you are creating the portal tablespace within an existing database, see [Section 4.1.1.3, "Creating the Portal Tablespace on Oracle Database for Microsoft Windows."](#)

---



---

The following must be done before scripting the database:

- Log in to the portal database host computer.
- Verify that ORACLE\_BASE, ORACLE\_HOME, and ORACLE\_SID are set appropriately. For details, see [Section 2.4, "Setting Oracle Environment Variables."](#)

- If this is a re-creation of a database or a retry of a prior failed attempt, delete the old database file.
1. Register the portal SID in the registry by running RegisterSIDPLUM.reg.  
RegisterSIDPLUM.reg is in the directory on the Oracle Database server to which you copied the scripts.
  2. Create and configure the portal database:
    - a. Create the PLUM directory under %ORACLE\_BASE%\oradata.
    - b. Copy initPLUM.ora to %ORACLE\_HOME%\database.
  3. Run CreateService.bat with the argument PLUMpassword.
  4. Create the portal database instance:
    - a. From %ORACLE\_BASE%\admin\%ORACLE\_SID%\plumtreescripts, start sqlplus using the /nolog parameter.
    - b. Run the crdb1\_oracle\_nt.sql script to create and start the new database instance.  
  
This script should generate no errors. Output from the script is saved in the file crdb1.lst in the plumtree scripts directory. The database should now be running.
    - c. Verify that the correct data files have been created.  
  
In %ORACLE\_BASE%\database you should see the following:
 

```
systPLUM.dbf
undo1A.dbf
temp1A.dbf (single disk installation only.)
```
  5. Create the portal tablespace and user:
    - a. Run the crdb2\_oracle\_nt.sql script to create tablespaces, create the portal database user, and perform low level database tuning.  
  
This script can take a significant amount of time to complete. The process may generate the following errors:
 

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

  
These errors are acceptable. Any other errors are not acceptable. Output from the script is saved in the file crdb1.lst in the plumtree scripts directory.
    - b. Verify that the correct data files have been created.  
  
In %ORACLE\_BASE%\database you should see the following:
 

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

#### 4.1.1.2 Creating the Portal Database on Oracle Database 10g or 11g for Microsoft Windows

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

---



---

**Note:** These steps create a new, dedicated portal database. If you are creating the portal tablespace within an existing database, see [Section 4.1.1.3, "Creating the Portal Tablespace on Oracle Database for Microsoft Windows."](#)

---



---

The following must be done before scripting the database:

- Log in to the portal database host computer.
  - Verify that ORACLE\_BASE, ORACLE\_HOME, and ORACLE\_SID are set appropriately. For details, see [Section 2.4, "Setting Oracle Environment Variables."](#)
  - If this is a re-creation of a database or a retry of a prior failed attempt, delete the old database file.
1. Register the portal SID in the registry by running RegisterSIDPLUM10.reg.  
RegisterSIDPLUM10.reg is in the directory on the Oracle Database server to which you copied the scripts.
  2. Create and configure the portal database:
    - a. Create the PLUM directory under %ORACLE\_BASE%\oradata.
    - b. Copy initPLUM10.ora to %ORACLE\_HOME%\database.
  3. Run CreateService.bat with the argument PLUM10 password.
  4. Create the portal database instance.
    - a. From %ORACLE\_BASE%\admin%\ORACLE\_SID%\plumtreescripts, start sqlplus using the /nolog parameter.
    - b. Run the crdb1\_oracle\_nt.sql script to create and start the new database instance.  
  
This script should generate no errors. Output from the script is saved in the file crdb1.lst in the plumtree scripts directory. The database should now be running.
    - c. Verify that the correct data files have been created.  
  
In %ORACLE\_BASE%\database you should see the following:
 

```
systPLUM.dbf
undo1A.dbf
temp1A.dbf (single disk installation only.)
```
  5. Create the portal tablespace and user:
    - a. Run the crdb2\_oracle\_nt.sql script to create tablespaces, create the portal database user, and perform low level database tuning.  
  
This script can take a significant amount of time to complete. The process may generate the following errors:
 

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

  
These errors are acceptable. Any other errors are not acceptable. Output from the script is saved in the file crdb1.lst in the plumtree scripts directory.
    - b. Verify that the correct data files have been created.  
  
In %ORACLE\_BASE%\database you should see the following:



```

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

```

### 4.1.1.3 Creating the Portal Tablespace on Oracle Database for Microsoft Windows

---

**Note:** These steps create the portal tablespace within an existing database. If you are creating a new, dedicated portal database, see [Section 4.1.1.4, "Creating the Portal Schema on Oracle Database for Microsoft Windows."](#)

---

- Log in to the portal database host computer as the owner of the Oracle system files.
  - Verify that ORACLE\_BASE, ORACLE\_HOME, and ORACLE\_SID are set appropriately. For details, see [Section 2.4, "Setting Oracle Environment Variables."](#)
1. Connect to your database as a user with sysdba rights.
  2. Create the portal tablespace and DB user:
    - a. From %ORACLE\_BASE%\admin\\${ORACLE\_SID}\plumtreescripts, start sqlplus using the /nolog parameter.
    - b. Run the create\_ali\_tablespace\_nt.sql script to create the portal tablespace.
    - c. Run the create\_ali\_user\_oracle.sql script to create the portal schema user

### 4.1.1.4 Creating the Portal Schema on Oracle Database for Microsoft Windows

before creating the portal schema you must configure the database, tablespace, and database user. For details on Oracle9i, see [Section 4.1.1.1, "Creating the Portal Database on Oracle9i for Microsoft Windows."](#) For details on Oracle Database 10g, see [Section 4.1.1.2, "Creating the Portal Database on Oracle Database 10g or 11g for Microsoft Windows."](#)

This section describes how to create the portal schema.

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

```

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

```

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

Create the Oracle WebCenter Interaction tables, indexes, and stored procedures by running the init\_ali\_db\_oracle.sql script. This script must be run as the portal database user you created.

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

- create\_tables\_oracle.lst
- stored\_procs\_oracle.lst
- load\_seed\_info.lst
- postinst.lst

3. (Optional) Create an Oracle SPFILE.  
For the benefits of using an SPFILE, refer to Oracle documentation. To create the SPFILE, run the `create_spfile_oracle_nt.sql` script.
4. Create the ALUI Directory tables.  
Run the following scripts in order:
  - a. `create_tables.sql`
  - b. `create_functions.sql`
  - c. `map_wcidb_103.sql`

## 4.1.2 Creating and Configuring the Portal Database on Microsoft SQL Server

This section provides an overview of how to create and configure the Oracle WebCenter Interaction portal database on Microsoft SQL Server.

1. Create and configure the portal database.  
For details, see [Section 4.1.2, "Creating and Configuring the Portal Database on Microsoft SQL Server"](#).
2. Script the portal database.  
For details, see [Section 4.1.2.2, "Scripting the Portal Database on Microsoft SQL Server"](#)

### 4.1.2.1 Creating and Configuring the Portal Database on Microsoft SQL Server

This section describes how to create and configure the portal database on Microsoft SQL Server 2005.

1. Configure the SQL Server instance to use **SQL Server and Windows Authentication mode**.
2. Create the portal database.
  - a. Set the portal database name to the name you specified in the Configuration Manager while completing installation for Oracle WebCenter Interaction.
  - b. Verify that the initial size of the portal database is sufficient for your Oracle WebCenter Interaction deployment.  
  
For a relatively small installation, configure a database that is at least 100 MB. For a large enterprise with as many as 20,000 users, configure a database that is as large as 1 GB.
  - c. Choose a case-insensitive collation, such as `SQL_Latin1_General_CP1_CI_AS`.
3. Create the portal database user.
  - a. Create the portal database user with the user name and password you specified when you ran the Oracle WebCenter Interaction installer.
  - b. Configure the portal database user to use **SQL Server Authentication**.
  - c. Set the portal database user's default database to the portal database.
4. Grant the portal database user the `db_owner` role for the portal database.

### 4.1.2.2 Scripting the Portal Database on Microsoft SQL Server

This section describes how to create and populate SQL Server tables necessary for the Oracle WebCenter Interaction portal.

We recommend that you run the scripts as the sa user so that the tables are owned by dbo.

---

**Note:** See Knowledge Base article 778539.1 for a discussion of the benefits of dbo object ownership.

---

1. Delete previous tables (if they exist) and create the tables required for the new portal components by running the following script: *install\_dir\ptportal\10.3.3\sql\mssql\create\_tables\_mssql.sql*.
2. Create the portal objects required by the portal by running the following script: *install\_dir\ptportal\10.3.3\sql\mssql\load\_seed\_info\_mssql.sql*
3. Create the stored procedures required by the portal by running the following script: *install\_dir\ptportal\10.3.3\sql\mssql\stored\_procs\_mssql.sql*
4. If your imageserver is located on a computer other than the one hosting your portal server, use a text editor to edit the *postinst\_mssql.sql* file to correctly reflect the imageserver location. Find the following setting, and replace *server* with the new location:

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

5. Set configuration information required by the portal by running the following script: *install\_dir\ptportal\10.3.3\sql\mssql\postinst\_mssql.sql*.
6. Run the SQL scripts for ALUI Directory.

The scripts are located in *install\_dir\aluidirectory\1.1\sql\mssql*. Run the scripts in the following order:

- a. *create\_tables.sql*
- b. *create\_functions.sql*
- c. *map\_alidb\_65.sql*

---

**Note:** The *create\_functions.sql* and *map\_alidb\_65.sql* scripts assume that all portal tables are under DBO. If your portal tables are under a different schema, you must manually edit *create\_functions.sql* and *map\_alidb\_65.sql*, making the following replacements:

- DBO . PTAUTHSOURCES must be changed to *your\_schema . PTAUTHSOURCES*
- DBO . LDAP\_ORG\_UNITS must be changed to *your\_schema . LDAP\_ORG\_UNITS*

For more information on handling portal objects that are not in the DBO schema, refer to *install\_dir\aluidirectory\1.1\sql\mssql\README.txt*.

---

## 4.2 Creating and Configuring the Notification Service Database

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

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

To configure an external database:

1. Script your database.
  - For details on scripting an Oracle database, see [Section 4.2.1, "Creating an External Notification Database on Oracle Database."](#)
  - For details on scripting a Microsoft SQL Server database, see [Section 4.2.2, "Creating an External Notification Database on Microsoft SQL Server."](#)
2. Update Notification database configuration information in Configuration Manager.

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

## 4.2.1 Creating an External Notification Database on Oracle Database

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

- Log in to the portal database host computer as the owner of the Oracle system files. Unless otherwise noted, scripts must be run as the system user.
- Verify that `ORACLE_BASE`, `ORACLE_HOME`, and `ORACLE_SID` are set appropriately. For details, see [Section 2.4, "Setting Oracle Environment Variables."](#)

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

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

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

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

## 4.2.2 Creating an External Notification Database on Microsoft SQL Server

This section describes how to create and configure a Microsoft SQL Server database for the Notification service.

The script files referred to in the following steps are found in `install_dir\cns\1.1\sql\mssql`.

1. Create a new database for the Notification service.

2. Give a user the db\_owner role on the new database.  
Create a new database user for the Notification service, or use an existing user.
3. Run cns-createTables.sql.
4. Run cns-data.sql.

## 4.3 Creating and Configuring the Tagging Engine Database

This section describes how to create and configure a database for the Tagging Engine. 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_tablespace.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. You were required to create the ALUI Security database when you installed Oracle WebCenter Analytics.

---

### 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.
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.





---

---

## Postinstallation Tasks

This chapter describes how to start the Oracle WebCenter Interaction services, run the diagnostics script, start the portal, and import migration packages into the portal.

The steps must be performed in the following order:

1. [Starting the Oracle WebCenter Interaction Services](#)
2. [Running the Diagnostics Script](#)
3. [Starting the Portal](#)
4. [Importing Migration Packages](#)

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

- If you installed the Tagging Engine, complete the tasks described in [Appendix A, "Completing Installation of the Tagging Engine."](#)
- If you installed the Oracle WebCenter Interaction Content Service for Documentum, complete the tasks described in [Appendix B, "Completing Installation of Oracle WebCenter Interaction Content Service for Documentum."](#)
- If you installed the Oracle WebCenter Interaction Content Service for Oracle Universal Content Management, complete the tasks described in [Appendix C, "Completing Installation of Oracle WebCenter Content Service for Oracle Universal Content Management."](#)
- If you installed the Oracle WebCenter Interaction Content Service for Lotus Notes, complete the tasks described in [Appendix D, "Completing Installation 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 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 of Oracle WebCenter Interaction Identity Service for Microsoft Active Directory."](#)

- If you installed the Oracle WebCenter Interaction Console for SharePoint, complete the tasks described in [Appendix J, "Completing Installation of Oracle WebCenter Console for Microsoft SharePoint."](#)

## 5.1 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. Navigate 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.
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.

## 5.2 Running the Diagnostics Script

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

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

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

- Run the diagnostics script, *install\_dir\ptportal\10.3.3\bin\diagnostic.bat*

---

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

---

## 5.3 Starting the Portal

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

To start the portal:

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

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

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

---

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

---

## 5.4 Importing Migration Packages

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

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

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

Import the migration packages relevant to your installation:

- Import the Search Cluster Manager, import the migration package located in *install\_dir\ptsearchserver\10.3.3\serverpackages*:
  - SearchClusterAdminUI.ptc

---

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

---

- If you installed the Content Upload service, import the migration package located in *install\_dir\ptupload\10.3.3\serverpackages*:
  - contentupload.ptc

- If you installed the Remote Portlet Service, import the migration packages located in *install\_dir*\remoteps\1.1\serverpackages:
  - activityservice.pte
  - EnterprisePoke.pte
  - KnowledgeDirectoryPortlet.pte
  - MyPictureProfilePortlet.pte
  - PostedLinksPortlet.pte
  - ProfilePortlets.pte
  - RSSReader.pte
  - RSSContentTypesAndProperties.pte
  - RSSTypeMapAndPropertyMap\_Global.pte
- If you installed the Notification service, import the migration package located in *install\_dir*\cns\1.1\serverpackages:
  - notification.pte
- If you installed the Tagging Engine, import the migration packages located in *install\_dir*\pathways\10.3.3\serverpackages:
  - TaggingEngine.pte
  - TaggingEngine\_autotag\_ext\_op.pte

This package add a job for automatically tagging objects in the Knowledge Directory.
- If you installed the Oracle WebCenter Interaction Content Service for Documentum, import the migration packages located in *install\_dir*\ptdctmcws\10.3.3\serverpackages:
  - DocumentumCS.pte
  - GlobalDocumentTypeMapDocumentum.pte
- If you installed the Oracle WebCenter Content Service for Oracle Universal Content Management, import the migration package located in *install\_dir*\ptucmcws\10.3.3\serverpackages:
  - UCMCS\_WS\_RemoteServer.pte
- If you installed the Oracle WebCenter Interaction Content Service for Lotus Notes, import the migration packages located in *install\_dir*\ptnotescws\10.3.3\serverpackages\\*:
  - LotusNotesCS\_WS\_RemoteServer.pte
  - LotusNotesCS\_DocumentType.pte
- If you installed the Oracle WebCenter Interaction Content Service for Windows Files, import the migration package located in *install\_dir*\ptntcws\10.3.3\serverpackages\\*:
  - WindowsFilesCS\_WS\_RemoteServer.pte
- If you installed the Oracle WebCenter Interaction Content Service for Microsoft Exchange, import the migration packages located in *install\_dir*\ptexchange\10.3.3\serverpackages\\*:
  - ExchangeWSOAndRemoteServer.pte

- MExchangeCrawlerGlobalObjects.pte
- If you installed the Oracle WebCenter Interaction Identity Service for LDAP, import the migration package: located in *install\_dir*\ptldapaws\10.3.3\serverpackages:
  - IdentityService-LDAP.pte
- If you installed the Oracle WebCenter Interaction Identity Service for Microsoft Active Directory, import the migration package located in *install\_dir*\ptadaws\10.3.3\serverpackages\
  - IdentityService-ActiveDirectory.pte
- If you installed the Oracle WebCenter JSR-168 Container, import the migration package located in *install\_dir*\ptjsr168\10.3.3\serverpackages:
  - jsr-168-samples.pte
- If you installed the Oracle WebCenter Console for Microsoft SharePoint, import the migration package located in *install\_dir*\ptsharepointcws\10.3.3\packages\
  - SharePoint\_Console.pte



---

---

# Completing Installation of the Tagging Engine

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

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

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

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

To seed the database:

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

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

## A.2 Configuring the Tag Me Portlet

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

To configure the Tag Me portlet:

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

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

## A.3 Troubleshooting

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

- [Overview of Tagging Engine Logs](#)
- [When to Use the Logging Utilities](#)

### A.3.1 Overview of Tagging Engine Logs

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

**Table A-1** Tagging Engine Installation Logs

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

### A.3.2 When to Use the Logging Utilities

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

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



---

---

## Completing Installation of Oracle WebCenter Interaction Content Service for Documentum

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

- [Section B.1, "Verifying Installation"](#)
- [Section B.2, "Creating a Content Source"](#)
- [Section B.3, "Creating a Content Crawler"](#)
- [Section B.4, "Creating a Job"](#)
- [Section B.5, "Configuring Security for Document Discovery"](#)
- [Section B.6, "Configuring Security for Document Access"](#)
- [Section B.7, "Setting the Preferred Document Rendition"](#)
- [Section B.8, "Advanced Configuration: Tuning Documentum Server"](#)
- [Section B.9, "Troubleshooting"](#)

### B.1 Verifying Installation

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

### B.2 Creating a Content Source

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

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

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

## B.3 Creating a Content Crawler

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

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

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

## B.4 Creating a Job

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

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

## B.5 Configuring Security for Document Discovery

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

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

---

---

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

---

---

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

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

**Table B-1** *accessLevelMapping Settings*

Setting	Description
<code>&lt;accessLevelMapping&gt;2&lt;/accessLevelMapping&gt;</code>	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).
<code>&lt;accessLevelMapping&gt;3&lt;/accessLevelMapping&gt;</code>	This value restricts portal document discovery to Documentum users that have at least Read access (Documentum Level 3 privilege).

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

---

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

---

Stay logged in to the portal for the next procedure.

## B.6 Configuring Security for Document Access

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



**Table B-2 Click-Through Security Methods**

Click-Through Security Method	Description and Procedure
User Preferences	<p>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.</p> <p>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 <code>clickthroughAuthType</code> as follows:</p> <pre>&lt;clickthroughAuthType&gt;1&lt;/clickthroughAuthType&gt;</pre> <p>When users click through to a Documentum file for the first time, they are prompted for their Documentum credentials. The portal stores the credentials as user preferences, so the user does not have to enter them again. Users can modify the values of these credentials by clicking <b>My Account</b>, then <b>Oracle WebCenter Interaction Content Service for Documentum</b>.</p>

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

Basic Authentication	<p>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.</p> <p><b>Note:</b> 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</p> <p>To enable Basic Authentication click-through:</p> <p>Disable User Preference click-through in the portal:</p> <ol style="list-style-type: none"> <li>1. In the portal's Administrative Object Directory, open the Oracle WebCenter Interaction Content Service for Documentum folder.</li> <li>2. Expand the Web Service section and click the <b>Oracle WebCenter Interaction Content Service for Documentum</b> Web service.</li> <li>3. On the left, under Edit Object Settings, click <b>Advanced URL Settings</b>.</li> <li>4. Remove the entry from the <b>User Configuration URL</b> box.</li> <li>5. On the left, under Edit Object Settings, click <b>Preferences</b>.</li> <li>6. Delete all User Preferences and click <b>Finish</b>.</li> </ol> <p>Stay logged in to the portal with the Oracle WebCenter Interaction Content Service for Documentum folder open for the next procedure.</p> <p>Enable Basic Authentication in the portal:</p> <ol style="list-style-type: none"> <li>1. In the portal PTConfig.xml file, set the CaptureBasicAuthenticationForPortlets parameter to <b>1</b>.</li> <li>2. In the Oracle WebCenter Interaction Content Service for Documentum folder of the portal's Administrative Object Directory, click the <b>Oracle WebCenter Interaction Content Service for Documentum</b> Web service.</li> <li>3. On the left, under Edit Object Settings, click <b>Authentication Settings</b>.</li> <li>4. Select <b>User's Basic Authentication Information</b>.</li> <li>5. Restart the portal application server.</li> </ol> <p>Enable Basic Authentication click-through on the Oracle WebCenter Interaction Content Service for Documentum host computer:</p> <ol style="list-style-type: none"> <li>1. In the Oracle WebCenter Interaction Content Service for Documentum config.xml file (located by default in C:\Oracle\Middleware\wci\ptdctmcws\10.3.3\settings\config), set clickthroughAuthType as follows:  <pre>&lt;clickthroughAuthType&gt;2&lt;/clickthroughAuthType&gt;</pre></li> </ol>
----------------------	---

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

Trusted Authentication	<p>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.</p> <p>To enable Trusted Authentication click-through:</p> <p>Disable User Preference click-through in the portal:</p> <ol style="list-style-type: none"> <li>1. In the portal's Administrative Object Directory, open the Oracle WebCenter Interaction Content Service for Documentum folder.</li> <li>2. Expand the Web Service section and click the <b>Oracle WebCenter Interaction Content Service for Documentum</b> Web service.</li> <li>3. On the left, under Edit Object Settings, click <b>Advanced URL Settings</b>.</li> <li>4. Remove the entry from the <b>User Configuration URL</b> box.</li> <li>5. On the left, under Edit Object Settings, click <b>Preferences</b>.</li> <li>6. Delete all User Preferences and click <b>Finish</b>.</li> </ol> <p>Stay logged in to the portal with the Oracle WebCenter Interaction Content Service for Documentum folder open for the next procedure.</p> <p>Enable Trusted Authentication click-through on the Oracle WebCenter Interaction Content Service for Documentum host computer:</p> <ol style="list-style-type: none"> <li>1. In the Oracle WebCenter Interaction Content Service for Documentum config.xml file (located by default in C:\Oracle\Middleware\wci\ptdctmcws\10.3.3\settings\config), set <code>clickthroughAuthType</code> as follows: <pre>&lt;clickthroughAuthType&gt;3&lt;/clickthroughAuthType&gt;</pre> </li> <li>2. In config.xml file, specify the following parameters for the SSO partner: <pre>&lt;trustedUserName&gt;&lt;/trustedUserName&gt; &lt;trustedPassword&gt;&lt;/trustedPassword&gt; &lt;trustedDomain&gt;&lt;/trustedDomain&gt;</pre> </li> </ol> <p><b>Note:</b> The value for the <code>&lt;trustedPassword&gt;</code> parameter must be encrypted. Use the <b>Encrypt Password</b> link located at:  <a href="http://RemoteServer:port/ptdctmcws/web/install/index.html">http://RemoteServer:port/ptdctmcws/web/install/index.html</a></p>
------------------------	--

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

Admin Preference/Content Source Credential	<p>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.</p> <p>To enable Super User click-through:</p> <p>Disable User Preference click-through in the portal:</p> <ol style="list-style-type: none"> <li>1. In the portal's Administrative Object Directory, open the Oracle WebCenter Interaction Content Service for Documentum folder.</li> <li>2. Expand the Web Service section and click the <b>Oracle WebCenter Interaction Content Service for Documentum</b> Web service.</li> <li>3. On the left, under Edit Object Settings, click <b>Advanced URL Settings</b>.</li> <li>4. Remove the entry from the <b>User Configuration URL</b> box.</li> <li>5. On the left, under Edit Object Settings, click <b>Preferences</b>.</li> <li>6. Delete all User Preferences and click <b>Finish</b>.</li> </ol> <p>Stay logged in to the portal with the Oracle WebCenter Interaction Content Service for Documentum folder open for the next procedure.</p> <p>Enable content source credential click-through on the Oracle WebCenter Interaction Content Service for Documentum host computer:</p> <ol style="list-style-type: none"> <li>1. In the Oracle WebCenter Interaction Content Service for Documentum config.xml file (located by default in C:\Oracle\Middleware\wci\ptdctmcws\10.3.3\settings\config), set <code>clickthroughAuthType</code> as follows: <pre>&lt;clickthroughAuthType&gt;4&lt;/clickthroughAuthType&gt;</pre> </li> </ol>
--	--

## B.7 Setting the Preferred Document Rendition

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

**Table B–3 Possible Preferred Rendition Format Element Values**

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

## B.8 Advanced Configuration: Tuning Documentum Server

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



---

---

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

---

---

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

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

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

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

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

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

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

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

## B.9 Troubleshooting

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

- [Reviewing Log Files](#)
- [Modifying Configuration Files](#)
- [Diagnosing Unexpected Results](#)

### B.9.1 Reviewing Log Files

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

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

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

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

## B.9.2 Modifying Configuration Files

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

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

**Table B-4 Configuration Parameters**

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

**Table B-4 (Cont.) Configuration Parameters**

Configuration (sample value in bold)	Value Description
<code>&lt;clickthroughAuthType&gt;<b>1</b>&lt;/clickthroughAuthType&gt;</code> <code>&lt;trustedUserName&gt;&lt;/trustedUserName&gt;</code> <code>&lt;trustedPassword&gt;&lt;/trustedPassword&gt;</code> <code>&lt;trustedDomain&gt;&lt;/trustedDomain&gt;</code>	<p>The clickthroughAuth type parameter determines what type of authentication to use during click-through. The following values are valid:</p> <ul style="list-style-type: none"> <li>■ 1 = User Preferences</li> <li>■ 2 = Basic Authentication</li> <li>■ 3 = Trusted Authentication</li> <li>■ 4 = Admin Preferences</li> </ul> <p>We recommend you set the accessLevelMapping value to 3 (read) if the clickThroughAuthType is either 4 or 5.</p> <p>See <a href="#">Section B.5, "Configuring Security for Document Discovery,"</a> for details on accessLevelMapping.</p> <p>For Trusted authentication (option #3), credentials must be supplied below. The password must be encrypted. Follow the instructions on <a href="http://RemoteServer/ptdctmcws/web/install/index.html">http://RemoteServer/ptdctmcws/web/install/index.html</a> to generate an encrypted password.</p>
<code>&lt;accessLevelMapping&gt;<b>2</b>&lt;/accessLevelMapping&gt;</code>	<p>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).</p> <p>Valid values for this parameter are:</p> <ul style="list-style-type: none"> <li>■ 2 = Browse</li> <li>■ 3 = Read</li> </ul>
<code>&lt;preferredRenditionFormat&gt;<b>default</b>&lt;/preferredRenditionFormat&gt;</code>	<p>Set the preferredRenditionFormat to the desired format for the document to be returned during click-through. The portal supports the following formats:</p> <ul style="list-style-type: none"> <li>■ default (or blank): The document's native format</li> <li>■ pdf: Acrobat PDF</li> <li>■ msw8: Microsoft Word 97/2000</li> <li>■ crtext: Text (Windows)</li> </ul> <p>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.</p> <p>This option only applies if userCredentialClickThrough is set to true.</p>

### B.9.3 Diagnosing Unexpected Results

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

**Table B-5 Troubleshooting**

Symptom	Solution
<p>HTTP 500 Error on Clickthrough</p> <p>Users have reported that the URL property in a document's Properties page is clickable, but the link returns an error.</p> <p>The URL property is unique as it is clickable in the Document Properties page (accessed by clicking <b>Properties</b> 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.</p>	<p>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.</p>
<p>Crawl fails with [DM_API_E_NO_SESSION] error: "There are no more available sessions."</p>	<p>Increase the sessions in server.ini and dmcl.ini. For details, see <a href="#">Section B.8, "Advanced Configuration: Tuning Documentum Server"</a>.</p>
<p>Port conflict, port in use, BindException</p>	<p>Port numbers for HTTP and HTTPS are configured in <i>install_dir</i>\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.</p>
<p>Memory consumption, Out of Memory Errors</p>	<p>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 <i>install_dir</i>\ptdctmcws\10.3.3\settings\config\wrapper.conf. For example, the following line shows a maximum memory setting of 1 GB:</p> <pre>wrapper.java.maxmemory=1024</pre> <p>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.</p>



---

---

# 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:

- [Section C.1, "Verifying Installation"](#)
- [Section C.2, "Creating a Content Source"](#)
- [Section C.3, "Creating a Content Crawler"](#)
- [Section C.4, "Creating a Job"](#)
- [Section C.5, "Configuring Security for Document Discovery"](#)
- [Section C.6, "Configuring Security for Document Access"](#)
- [Section C.7, "Troubleshooting"](#)

## C.1 Verifying Installation

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

## C.2 Creating a Content Source

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

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

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

### C.3 Creating a Content Crawler

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

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

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

### C.4 Creating a Job

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

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

### C.5 Configuring Security for Document Discovery

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

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

---

---

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

---

---



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

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

Stay logged in to the portal for the next procedure.

## C.6 Configuring Security for Document Access

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



**Table C-1 Click-Through Security Methods**

Click-Through Security Method	Description and Procedure
User Preferences	<p>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.</p> <p>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 <code>clickthroughAuthType</code> as follows:</p> <pre data-bbox="581 554 1149 579">&lt;clickthroughAuthType&gt;1&lt;/clickthroughAuthType&gt;</pre> <p>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 <b>My Account</b>, then <b>Oracle WebCenter Content Service for UCM</b>.</p>

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

Basic Authentication	<p>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.</p> <p><b>Note:</b> 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</p> <p>To enable Basic Authentication click-through:</p> <p>Disable User Preference click-through in the portal:</p> <ol style="list-style-type: none"> <li>1. In the portal's Administrative Object Directory, open the Oracle WebCenter Content Service for UCM folder.</li> <li>2. Expand the Web Service section and click the <b>Oracle WebCenter Content Service for UCM</b> Web service.</li> <li>3. On the left, under Edit Object Settings, click <b>Advanced URL Settings</b>.</li> <li>4. Remove the entry from the <b>User Configuration URL</b> box.</li> <li>5. On the left, under Edit Object Settings, click <b>Preferences</b>.</li> <li>6. Delete all User Preferences and click <b>Finish</b>.</li> </ol> <p>Stay logged in to the portal with the Oracle WebCenter Content Service for UCM folder open for the next procedure.</p> <p>Enable Basic Authentication in the portal:</p> <ol style="list-style-type: none"> <li>1. In the portal PTConfig.xml file, set the CaptureBasicAuthenticationForPortlets parameter to <b>1</b>.</li> <li>2. In the Oracle WebCenter Content Service for UCM folder of the portal's Administrative Object Directory, click the <b>Oracle WebCenter Content Service for UCM</b> Web service.</li> <li>3. On the left, under Edit Object Settings, click <b>Authentication Settings</b>.</li> <li>4. Select <b>User's Basic Authentication Information</b>.</li> <li>5. Restart the portal application server.</li> </ol> <p>Enable Basic Authentication click-through on the Oracle WebCenter Content Service for Oracle Universal Content Management host computer:</p> <ol style="list-style-type: none"> <li>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:  &lt;clickthroughAuthType&gt;2&lt;/clickthroughAuthType&gt;</li> </ol>
----------------------	--

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

Trusted Authentication	<p>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.</p> <p>To enable Trusted Authentication click-through:</p> <p>Disable User Preference click-through in the portal:</p> <ol style="list-style-type: none"> <li>1. In the portal's Administrative Object Directory, open the Oracle WebCenter Content Service for UCM folder.</li> <li>2. Expand the Web Service section and click the <b>Oracle WebCenter Content Service for UCM</b> Web service.</li> <li>3. On the left, under Edit Object Settings, click <b>Advanced URL Settings</b>.</li> <li>4. Remove the entry from the <b>User Configuration URL</b> box.</li> <li>5. On the left, under Edit Object Settings, click <b>Preferences</b>.</li> <li>6. Delete all User Preferences and click <b>Finish</b>.</li> </ol> <p>Stay logged in to the portal with the Oracle WebCenter Content Service for UCM folder open for the next procedure.</p> <p>Enable Trusted Authentication click-through on the Oracle WebCenter Content Service for Oracle Universal Content Management host computer:</p> <ol style="list-style-type: none"> <li>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 <code>clickthroughAuthType</code> as follows: <pre>&lt;clickthroughAuthType&gt;3&lt;/clickthroughAuthType&gt;</pre> </li> <li>2. In config.xml file, specify the following parameters for the SSO partner: <pre>&lt;trustedUserName&gt;&lt;/trustedUserName&gt; &lt;trustedPassword&gt;&lt;/trustedPassword&gt; &lt;trustedDomain&gt;&lt;/trustedDomain&gt;</pre> </li> </ol> <p><b>Note:</b> The value for the <code>&lt;trustedPassword&gt;</code> parameter must be encrypted. Use the <b>Encrypt Password</b> link located at:  <a href="http://RemoteServer:port/ptdctmcws/web/install/index.html">http://RemoteServer:port/ptdctmcws/web/install/index.html</a></p>
------------------------	--

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

Admin Preference/Content Source Credential	<p>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.</p> <p>To enable Super User click-through:</p> <p>Disable User Preference click-through in the portal:</p> <ol style="list-style-type: none"> <li>1. In the portal's Administrative Object Directory, open the Oracle WebCenter Content Service for UCM folder.</li> <li>2. Expand the Web Service section and click the <b>Oracle WebCenter Content Service for UCM Web service</b>.</li> <li>3. On the left, under Edit Object Settings, click <b>Advanced URL Settings</b>.</li> <li>4. Remove the entry from the <b>User Configuration URL</b> box.</li> <li>5. On the left, under Edit Object Settings, click <b>Preferences</b>.</li> <li>6. Delete all User Preferences and click <b>Finish</b>.</li> </ol> <p>Stay logged in to the portal with the Oracle WebCenter Content Service for UCM folder open for the next procedure.</p> <p>Enable content source credential click-through on the Oracle WebCenter Content Service for Oracle Universal Content Management host computer:</p> <ol style="list-style-type: none"> <li>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 <code>clickthroughAuthType</code> as follows:  <pre>&lt;clickthroughAuthType&gt;4&lt;/clickthroughAuthType&gt;</pre> </li> </ol>
--	---

## C.7 Troubleshooting

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

- [Reviewing Log Files](#)
- [Modifying Configuration Files](#)
- [Diagnosing Unexpected Results](#)

### C.7.1 Reviewing Log Files

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

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

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

## C.7.2 Modifying Configuration Files

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

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

**Table C-2 Configuration Parameters**

<b>Configuration (sample value in bold)</b>	<b>Value Description</b>
baseURL	<p>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.</p> <p>When you configure Oracle WebCenter Interaction applications, always specify the fully qualified domain name for hosts to avoid host and domain name resolution mismatches.</p>



**Table C-2 (Cont.) Configuration Parameters**

Configuration (sample value in bold)	Value Description
<code>&lt;clickthroughAuthType&gt;<b>1</b>&lt;/clickthroughAuthType&gt;</code> <code>&lt;trustedUserName&gt;&lt;/trustedUserName&gt;</code> <code>&lt;trustedPassword&gt;&lt;/trustedPassword&gt;</code> <code>&lt;trustedDomain&gt;&lt;/trustedDomain&gt;</code>	<p>The clickthroughAuth type parameter determines what type of authentication to use during click-through. The following values are valid:</p> <ul style="list-style-type: none"> <li>■ 1 = User Preferences</li> <li>■ 2 = Basic Authentication</li> <li>■ 3 = Trusted Authentication</li> <li>■ 4 = Admin Preferences</li> </ul> <p>We recommend you set the accessLevelMapping value to 3 (read) if the clickThroughAuthType is either 4 or 5.</p> <p>See <a href="#">Section C.5, "Configuring Security for Document Discovery,"</a> for details on accessLevelMapping.</p> <p>For Trusted authentication (option #3), credentials must be supplied below. The password must be encrypted. Follow the instructions on <a href="http://RemoteServer/ptucmcws/web/install/index.html">http://RemoteServer/ptucmcws/web/install/index.html</a> to generate an encrypted password.</p>
<code>&lt;accessLevelMapping&gt;<b>2</b>&lt;/accessLevelMapping&gt;</code>	<p>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).</p> <p>Valid values for this parameter are:</p> <ul style="list-style-type: none"> <li>■ 2 = Browse</li> <li>■ 3 = Read</li> </ul>
<code>&lt;preferredRenditionFormat&gt;<b>default</b>&lt;/preferredRenditionFormat&gt;</code>	<p>Set the preferredRenditionFormat to the desired format for the document to be returned during click-through. The portal supports the following formats:</p> <ul style="list-style-type: none"> <li>■ default (or blank): The document's native format</li> <li>■ pdf: Acrobat PDF</li> <li>■ msw8: Microsoft Word 97/2000</li> <li>■ crtext: Text (Windows)</li> </ul> <p>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.</p> <p>This option only applies if userCredentialClickThrough is set to true.</p>

### 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
<p>HTTP 500 Error on Clickthrough</p> <p>Users have reported that the URL property in a document's Properties page is clickable, but the link returns an error.</p> <p>The URL property is unique as it is clickable in the Document Properties page (accessed by clicking <b>Properties</b> 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.</p>	<p>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.</p>
<p>Port conflict, port in use, BindException</p>	<p>Port numbers for HTTP and HTTPS are configured in <i>install_dir\ptdctmcws\10.3.3\settings\config\application.conf</i>. 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.</p>
<p>Memory consumption, Out of Memory Errors</p>	<p>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 <i>install_dir\ucmcws\10.3.3\settings\config\wrapper.conf</i>. For example, the following line shows a maximum memory setting of 1 GB:</p> <pre>wrapper.java.maxmemory=1024</pre> <p>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.</p>

# D

---

---

## Completing Installation of Oracle WebCenter Interaction Content Service for Lotus Notes

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

- [Section D.1, "Verifying Installation"](#)
- [Section D.2, "Configuring Security"](#)
- [Section D.3, "Creating a Content Source"](#)
- [Section D.4, "Creating a Content Crawler"](#)
- [Section D.5, "Creating a Job"](#)
- [Section D.6, "Configuring User Preferences for Click-Through"](#)
- [Section D.7, "Configuring Remote Server Logging"](#)

### D.1 Verifying Installation

To verify a successful installation:

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

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, ensure that 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 Click-Through

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*

---

---



---

---

## Completing Installation of Oracle WebCenter Interaction Content Service for Windows Files

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

- [Section E.1, "Setting Up Security Rights for Oracle WebCenter Interaction Content Service for Windows Files"](#)
- [Section E.2, "Verifying the Security Library"](#)
- [Section E.3, "Configuring Security"](#)
- [Section E.4, "Creating a Content Source"](#)
- [Section E.5, "Creating a Content Crawler"](#)
- [Section E.6, "Creating a Job"](#)
- [Section E.7, "Advanced Configuration"](#)

---

---

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

---

---

### 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

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\Middleware\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.

---

---

# Completing Installation of Oracle WebCenter Interaction Content Service for Microsoft Exchange

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

- [Section F.1, "Configuring Security"](#)
- [Section F.2, "Creating a Content Source"](#)
- [Section F.3, "Creating a Content Crawler"](#)
- [Section F.4, "Creating a Job"](#)

## F.1 Configuring Security

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 2.9, "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**.



---

---

# Completing Installation of Oracle WebCenter Interaction Identity Service for LDAP

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

- [Verifying Installation](#)
- [Creating a Remote Authentication Source](#)
- [Creating a Remote Profile Source](#)
- [Creating a Job](#)

This chapter also include the section [Section G.5, "Advanced Configuration,"](#) which includes the following optional advanced procedures for LDAP configuration:

- [Configuring Logging](#)
- [Configuring Application Server Session Settings](#)
- [Configuring LDAP Server Settings](#)
- [Using Oracle WebCenter Interaction Identity Service for LDAP over SSL](#)

## G.1 Verifying Installation

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

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

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

## G.2 Creating a Remote Authentication Source

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

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

4. From the **Create Object** menu, choose **Authentication Source - Remote**.
  5. In the Choose Web Service dialog box, choose **LDAP IDS**.
  6. Configure the authentication source as described in the online help.
- Stay logged in to the portal with the LDAP IDS folder open for the next procedure.

## G.3 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.4 Creating a Job

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

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

## G.5 Advanced Configuration

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

- [Configuring Logging](#)
- [Configuring Application Server Session Settings](#)
- [Configuring LDAP Server Settings](#)
- [Using Oracle WebCenter Interaction Identity Service for LDAP over SSL](#)

### G.5.1 Configuring Logging

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

There are two appenders defined:



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

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

**Table 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 <code>RollingFileAppender</code> .  If you choose to roll over based on the date, the <code>MaxFileSize</code> 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 <code>MaxBackupIndex</code> value depends on how much disk space you choose to devote to log files.
DatePattern	Determines the basis on which files are rolled over if the appender is a <code>DailyRollingFileAppender</code> . <code>YYY-mm</code> means the file is rolled over once a month. <code>YYYY-mm-dd</code> means the file is rolled over every day. <code>YYYY-mm-dd-HH</code> rolls over every hour and so forth.
RollingFileAppender	If several synchronization jobs are run once a day use the <code>RollingFileAppender</code> so that the individual log files do not grow excessively large.
DailyRollingFileAppender	In changing the <code>DailyRollingFileAppender</code> from <code>RollingFileAppender</code> , the <code>MaxFileSize</code> setting is ignored. This enables you to set the type of appender to either rollover based on date or size.  If you use a <code>DailyRollingFileAppender</code> 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 <code>MaxBackupIndex</code> to 10 provides approximately two months of job histories.

## G.5.2 Configuring Application Server Session Settings

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

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

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

## G.5.3 Configuring LDAP Server Settings

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

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

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

- [Setting Up SSL Between the Portal and the Remote Server](#)
- [Setting Up SSL Between the Remote Server and the LDAP Server](#)

### G.5.4.1 Setting Up SSL Between the Portal and the Remote Server

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

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

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

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

### G.5.4.2 Setting Up SSL Between the Remote Server and the LDAP Server

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

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

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

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

---

---

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

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

- [Verifying Installation](#)
- [IIS Virtual Directory Settings](#)
- [Windows Installation Directory Settings](#)
- [Create a Remote Authentication Source](#)
- [Create a Remote Profile Source](#)
- [Creating a Job](#)

This chapter also includes the section [Section H.7, "Advanced Configuration"](#) which includes the following optional advanced procedures for Microsoft Active Directory configuration:

- [Editing the Web.config File](#)
- [Active Directory Server Query Timeouts](#)
- [Active Directory Errors During GetMembers](#)

## H.1 Verifying Installation

Verify installation 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 IIS Virtual Directory Settings

To edit virtual directory timeout 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.7.1, "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 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.2, "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.4 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.5 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.6 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.7 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.7.1 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.7.1.1 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.7.1.2 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.7.1.3 Choosing An Appropriate Rolling Style

If several synchronization jobs are run a day, you may want 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.7.1.4 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 want to increase the number of rollover files to keep a history that exceeds ten days.

### H.7.1.5 Archiving Log Files

You may want to keep a permanent archive of all the logs on another computer, or simply want 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.7.1.6 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.2, "IIS Virtual Directory Settings,"](#) for details on setting this timeout value.

---

---

## H.7.2 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.7.3 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:

- [Section I.1, "Configure Remote Server"](#)
- [Section I.2, "Install the Oracle WebCenter JSR-168 Container Samples"](#)

## I.1 Configure Remote Server

Add the path to Oracle WebCenter JSR-168 Container PT\_HOME:

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

---

---

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

---

---

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

## I.2 Install the Oracle WebCenter JSR-168 Container Samples

To install the Oracle WebCenter JSR-168 Container samples:

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

The Oracle WebCenter JSR-168 Container server package is *install\_dir\ptjsr168\10.3.3\serverpackages\jsr-168.pte*.

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

---

---

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

---

---

---

---

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

---

---

---

---

# Completing Installation of Oracle WebCenter Console for Microsoft SharePoint

If you installed Oracle WebCenter Console for Microsoft SharePoint, perform the following tasks to complete the installation:

- [Section J.1, "Verifying Installation"](#)
- [Section J.2, "Creating a Content Source"](#)
- [Section J.3, "Creating a Content Crawler"](#)
- [Section J.4, "Creating a Job"](#)

## J.1 Verifying Installation

To verify the Oracle WebCenter Console for Microsoft SharePoint service components have been installed, use the Windows Internet Information Services Manager to verify the Oracle WebCenter Console for Microsoft SharePoint virtual directories have been installed.

1. From Administrative Tools, open the **Internet Information Services Manager**.
2. In the IIS Web site you specified when installing the Oracle WebCenter Console for Microsoft SharePoint, these three virtual directories should be present: **SharePointCWS**, **CustomSearch**, and **SiteFeed**.

## J.2 Creating a Content Source

Oracle WebCenter Console for Microsoft SharePoint comes with a default content source, SharePoint Content Source, that can be updated with your MOSS or WSS information. To edit the content source, perform the following steps in the Oracle WebCenter Console for Microsoft SharePoint 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 Console for Microsoft SharePoint folder.
4. Open the SharePoint Content Source object.
5. Under SharePoint User Settings, enter the login information for a user that has access to all of the Microsoft SharePoint content that you wish to crawl into the portal. If the crawler will use a site feed, the user must have access to each of the sites specified by the site feed.

When the crawler accesses the desired Microsoft SharePoint site, it will run as this user. The user must have the following rights on the site:

- **Microsoft Office SharePoint Server 2007:** Browse Directories, Manage Lists, Use Remote Interfaces
- **Windows SharePoint Services 2.0:** Browse Directories, Manage List Permissions
- **Windows SharePoint Services 3.0:** Browse Directories, Manage Lists, Use Remote Interfaces

To crawl Form Template folders in MOSS 2007 and WSS 3.0, the View Application Pages and View Versions rights are also required.

---

---

**Note:** The authentication information configured in the content source is used only by the crawler. These credentials will not be passed to the Microsoft SharePoint site when a user clicks on an item in the portal. Authentication of the user to access that item is handled by MOSS or WSS.

---

---

6. If necessary, change other settings as described in the online help.

---

---

**Caution:** Do not change the gateway setting. The portal cannot gateway Microsoft SharePoint documents. The gateway interferes with authentication and WebDAV features of Microsoft SharePoint.

---

---

Stay logged in to the portal with the Oracle WebCenter Console for Microsoft SharePoint folder open for the next procedure.

### J.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 Console for Microsoft SharePoint 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, configure the SharePoint crawler settings:

**Table J-1 SharePoint Crawler Configuration - Main Settings**

Setting	Description
SharePoint Site	<p>Select <b>Site URL</b> to crawl a Microsoft SharePoint site or site collection. Type the URL of the site that you wish to crawl and click <b>Validate</b>. This URL should end in "/".</p> <ul style="list-style-type: none"> <li>■ The crawler will validate that the URL entered is a valid Microsoft SharePoint site or site collection and display the name of the starting subsite. If the URL entered does not end in "/" but a valid site collection can be extracted from the URL, the crawler will discard any extraneous trailing information from the URL and update the URL shown in the UI accordingly.</li> <li>■ The subsite name may be listed as "/" if the starting site is the root site of the site collection itself. If the starting Microsoft SharePoint URL points to a subsite of the site collection, the subsite will be listed.</li> </ul> <p>Select <b>Feed</b> to crawl a list of WSS sites specified by an RSS feed. Type the path to the site feed.</p> <ul style="list-style-type: none"> <li>■ The path must return a valid RSS 2.0 document. For more information about crawling RSS feeds, see <a href="#">Section J.4.1, "Crawling RSS Site Feeds."</a></li> </ul>
Crawl Depth	<p>Select the depth of the crawl.</p> <p>It is recommended that you choose <b>Selected Site and All Subsites</b> to simplify indexing of Microsoft SharePoint sites. If you do not choose this setting, you will have to create a separate crawler for each subsite. You should choose <b>Selected Site Only</b> if you want to tightly control what Microsoft SharePoint sites are indexed.</p>
Folder Path	Select the folder or folders where you would like to import Microsoft SharePoint content.
Settings	<p>Select how you would like to import the Microsoft SharePoint items.</p> <p>It is recommended that you choose to mirror the folder structure, approve imported documents, and import security. If you choose to mirror the folder structure, the crawler will mirror the Microsoft SharePoint site structure. Importing security means that only those users who can view the source item in MOSS or WSS can see the corresponding document in the portal and search results. For more information on importing security, see the <i>Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Interaction</i>.</p>
Document Access Privileges	Specify the access rights for the imported content.

4. On the **List Settings** page, check the box next to each type of Microsoft SharePoint item you want to crawl. To crawl documents attached to attached to the list items, select **Crawl documents attached to list items**.
5. Configure the remaining settings as described in the online help.

Stay logged in to the portal with the Oracle WebCenter Console for Microsoft SharePoint folder open for the next procedure.

## J.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 Console for Microsoft SharePoint folder of the portal's Administrative Object Directory:

1. From the **Create Object** menu, select **Job**.
2. Click **Add Operation**.
3. Choose the content crawler that you created in the previous procedure.
4. Choose the scheduling values for the job and click **Finish**.

5. Name the job and click **OK**.
6. When you are finished creating the job, ensure that the Oracle WebCenter Console for Microsoft SharePoint folder is associated with an automation service. For assistance, see the online help under **Select Utilities**, then **Automation Service**.

### J.4.1 Crawling RSS Site Feeds

In addition to crawling Microsoft SharePoint sites and site collections, SharePoint content crawlers can also be used to import content from a list of sites provided by an RSS feed.

The path to a site feed can be a URL (<http://>, <file:///>), a local file path on the Microsoft SharePoint machine (`c:\feed.xml`), or a UNC file path on the Microsoft SharePoint network (`\\server\feeds\feed.xml`). Secured sites (<https://>) and FTP sites (<ftp://>) cannot be crawled.

When you install Oracle WebCenter Console for Microsoft SharePoint, the installer creates a virtual directory named **SiteFeed** that can be used to deploy a simple RSS feed. For example, you can put a well-formed, valid XML feed document or an `.aspx` file that generates a site feed into the `sitfeed` folder on the file system and then access it via HTTP.

The site feed document should conform to the RSS 2.0 specification. The link element of each item must contain the URL to a valid Microsoft SharePoint site. The title element of an item is optional. If provided, it should be a valid Knowledge Directory folder name, as it will be used as the Knowledge Directory folder name for the site for a mirroring crawl. If the title element is omitted, the folder name will be retrieve from the Microsoft SharePoint site for a mirroring crawl.

Example site feed document:

```
<?xml version="1.0" encoding="utf-8" ?>
<rss version="2.0">
  <channel>
    <title>SharePoint Site List</title>
    <link>#</link>
    <description>List of SharePoint sites to be crawled by
Oracle WebCenter Console for SharePoint </description>
    <item>
      <title>MOSS TeamSite at
mySPServer:17938/sites/MainSiteCollection</title>
    <link>http://mySPServer:17938/sites/MainSiteCollection/</link>
    </item>
    <item>
      <link>http://SharePointServer:9167/</link>
    </item>
  </channel>
</rss>
```

---

---

# 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

## B

---

BEA ALI Content Service for Documentum -  
Application Port wizard page, 3-3

## C

---

click-through preferences, D-3  
content crawlers  
    configuring, F-2  
    creating, D-2  
content sources  
    creating, D-2, F-2

## D

---

dmcl.ini file, 2-5  
Documentum CS installation certification page  
    location, B-1  
Documentum DFC Runtime Environment  
    configuring, 2-5

## F

---

feeds  
    crawling, J-3  
folder structure  
    mirroring, J-3  
Fully Qualified Domain Name wizard page, 3-3, 3-4

## G

---

Global ACL Sync Map, D-1

## H

---

hardware  
    minimum requirements, 2-2

## J

---

jobs  
    creating, D-2, F-2

## L

---

list settings, J-3

## M

---

Microsoft Outlook  
    configuring, 2-6

## R

---

remote server logging  
    configuring, D-3  
RSS feeds, J-3  
    crawling, J-4

## S

---

security  
    configuring, D-1, F-1  
security library  
    verifying, E-2  
site collections  
    crawling, J-3  
site URL, J-3  
sitedfeed virtual directory, J-4  
sites  
    crawling, J-3  
software  
    minimum requirements, 2-2  
subsites  
    crawling, J-3

## T

---

testing connectivity, 2-6

## U

---

UCM CS installation certification page location, C-1  
user preferences  
    configuring, D-3

## V

---

virtual directories  
    CustomSearch, J-1  
    SharePointCWS, J-1  
    sitedfeed, J-1

