

**Oracle® Fusion Middleware**  
Administrator's Guide for Oracle WebCenter  
11g Release 1 (11.1.1)  
**E12405-02**

July 2009

Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter, 11g Release 1 (11.1.1)

E12405-02

Copyright © 2007, 2009, Oracle and/or its affiliates. All rights reserved.

Primary Author: Rosie Harvey

Contributing Author: Peter Jacobsen, Promila Chitkara, Savita Thakur, Ingrid Snedecor, Michele Cyran

Contributors: Christian Hauser, Clayton Jung, Jeni Ferns, Manish Devgan, Nicolas Pombourcq, Pankaj Mittal, Paul Encarnacion, Paul Lin, Paul Spencer, Peter Moskovits, Pushkar Kapasi, Rahmathulla Baig, Sanjay Khanna, Ved Singh, Virad Gupta

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 software or related documentation 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 USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software 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 which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software 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> .....              | xxxiii |
| Audience .....                    | xxxiii |
| Documentation Accessibility ..... | xxxiii |
| Related Documents .....           | xxxiv  |
| Conventions .....                 | xxxiv  |

## Part I Understanding Oracle WebCenter

### 1 Introduction to Oracle WebCenter Administration

|        |   |      |
|--------|---|------|
| 1.1    | Introducing Oracle WebCenter .....                                | 1-1  |
| 1.2    | Oracle WebCenter Architecture .....                               | 1-2  |
| 1.2.1  | WebCenter Framework .....   | 1-2  |
| 1.2.2  | Application Developer Framework .....                             | 1-3  |
| 1.2.3  | WebCenter Web 2.0 Services .....                                  | 1-3  |
| 1.2.4  | WebCenter Composer .....  | 1-3  |
| 1.2.5  | WebCenter Spaces .....  | 1-3  |
| 1.2.6  | Portals .....   | 1-4  |
| 1.2.7  | Composite Applications .....                                      | 1-4  |
| 1.3    | Oracle WebCenter Topology .....                                   | 1-4  |
| 1.3.1  | Oracle WebCenter Managed Servers .....                            | 1-5  |
| 1.3.2  | Oracle WebCenter Startup Order .....                              | 1-6  |
| 1.3.3  | Oracle WebCenter External Dependencies .....                      | 1-6  |
| 1.3.4  | Oracle WebCenter Configuration Considerations .....               | 1-7  |
| 1.3.5  | Oracle WebCenter State and Configuration Persistence .....        | 1-8  |
| 1.3.6  | Oracle WebCenter Log File Locations .....                         | 1-9  |
| 1.4    | Oracle WebCenter Spaces .....                                     | 1-9  |
| 1.5    | Custom WebCenter Applications .....                               | 1-9  |
| 1.6    | Planning WebCenter Installations .....                            | 1-10 |
| 1.7    | Understanding the WebCenter 11g Installation .....                | 1-10 |
| 1.8    | Understanding Administrative Operations, Roles, and Tools .....   | 1-10 |
| 1.9    | Performance Monitoring and Diagnostics .....                      | 1-12 |
| 1.10   | WebCenter Application Deployment .....                            | 1-12 |
| 1.11   | Data Migration, Backup, and Recovery .....                        | 1-12 |
| 1.12   | Oracle WebCenter Administration Tools .....                       | 1-12 |
| 1.12.1 | Oracle Enterprise Manager Fusion Middleware Control Console ..... | 1-13 |

|          |  |      |
|----------|--|------|
| 1.12.1.1 | Displaying Fusion Middleware Control Console .....           | 1-13 |
| 1.12.2   | Oracle WebLogic Server Administration Console .....          | 1-13 |
| 1.12.3   | Oracle WebLogic Scripting Tool (WLST) .....                  | 1-14 |
| 1.12.3.1 | Running Oracle WebLogic Scripting Tool (WLST) Commands ..... | 1-15 |
| 1.12.4   | WebCenter Spaces Administration Pages .....                  | 1-16 |

## Part II Getting Started With Oracle WebCenter Administration

### 2 Getting WebCenter Spaces Up and Running

|     |   |     |
|-----|---|-----|
| 2.1 | Role of the Fusion Middleware Administrator .....               | 2-1 |
| 2.2 | Role of the WebCenter Spaces Administrator .....                | 2-2 |
| 2.3 | Installing WebCenter Spaces .....                               | 2-2 |
| 2.4 | Setting Up WebCenter Spaces for the First Time (Roadmap) .....  | 2-3 |
| 2.5 | Customizing WebCenter Spaces for the First Time (Roadmap) ..... | 2-4 |

### 3 Maintaining WebCenter Spaces

|     |   |     |
|-----|---|-----|
| 3.1 | Role of the Fusion Middleware Administrator .....               | 3-1 |
| 3.2 | Role of the WebCenter Spaces Administrator .....                | 3-2 |
| 3.3 | System Administration for WebCenter Spaces (Roadmap) .....      | 3-2 |
| 3.4 | Application Administration for WebCenter Spaces (Roadmap) ..... | 3-5 |

### 4 Getting Custom WebCenter Applications Up and Running

|     |  |     |
|-----|--|-----|
| 4.1 | Installing Oracle WebCenter and Oracle WebCenter Framework Libraries ..... | 4-1 |
| 4.2 | Deploying Custom WebCenter Applications for the First Time (Roadmap) ..... | 4-1 |

### 5 Maintaining Custom WebCenter Applications

|     |   |     |
|-----|---|-----|
| 5.1 | System Administration for Custom WebCenter Applications (Roadmap) ..... | 5-1 |
|-----|---|-----|

## Part III Basic Systems Administration for Oracle WebCenter

### 6 Starting Enterprise Manager Fusion Middleware Control

|     |   |     |
|-----|---|-----|
| 6.1 | Displaying Fusion Middleware Control Console .....                  | 6-1 |
| 6.2 | Navigating to the Home Page for WebCenter Spaces .....              | 6-2 |
| 6.3 | Navigating to the Home Page for Custom WebCenter Applications ..... | 6-5 |
| 6.4 | Navigating to Dependent Components .....                            | 6-7 |

### 7 Deploying WebCenter Applications

|         |   |     |
|---------|---|-----|
| 7.1     | Deploying Custom WebCenter Applications .....                                   | 7-1 |
| 7.1.1   | Understanding Custom WebCenter Application Deployment .....                     | 7-2 |
| 7.1.2   | Creating the .EAR File .....  | 7-2 |
| 7.1.3   | Creating and Provisioning a WebLogic Managed Server Instance .....              | 7-2 |
| 7.1.3.1 | Creating a WebLogic Managed Server Using the WLS Administration Console .....   | 7-3 |
| 7.1.3.2 | Creating a WebLogic Managed Server Using Fusion Middleware Control .....        | 7-8 |
| 7.1.3.3 | Creating and Provisioning a WebLogic Managed Server Using a Jython Script ..... | 7-9 |



|           |  |      |
|-----------|--|------|
| 7.1.4     | Creating and Registering the Metadata Service (MDS) Repository .....         | 7-11 |
| 7.1.4.1   | Creating an MDS Schema.....  | 7-11 |
| 7.1.4.2   | Registering an MDS Schema Using Fusion Middleware Control .....              | 7-15 |
| 7.1.4.3   | Registering an MDS Schema Using WLST .....                                   | 7-17 |
| 7.1.5     | Deploying a WebCenter Application to a WebLogic Managed Server Instance .... | 7-18 |
| 7.1.5.1   | Deploying Custom WebCenter Applications Using Oracle JDeveloper .....        | 7-19 |
| 7.1.5.2   | Deploying Custom WebCenter Applications Using Fusion Middleware Control..... | 7-19 |
| 7.1.5.3   | Deploying Custom WebCenter Applications Using WLST .....                     | 7-24 |
| 7.1.5.4   | Deploying WebCenter Applications Using the WLS Administration Console        | 7-26 |
| 7.1.6     | Transporting Customizations Between Environments .....                       | 7-29 |
| 7.1.7     | Configuring WebCenter Applications to Run in a Distributed Environment.....  | 7-29 |
| 7.2       | Undeploying Custom WebCenter Applications .....                              | 7-29 |
| 7.2.1     | Undeploying WebCenter Applications Using Fusion Middleware Control .....     | 7-29 |
| 7.2.2     | Undeploying WebCenter Applications Using WLST.....                           | 7-30 |
| 7.2.3     | Removing an Application's Credential Map .....                               | 7-30 |
| 7.3       | Redeploying Custom WebCenter Applications .....                              | 7-31 |
| 7.3.1     | Redeployment Considerations .....  | 7-32 |
| 7.3.1.1   | Preserving Application Configuration .....                                   | 7-32 |
| 7.3.1.1.1 | Preserving Configuration Across Deployment Using WLST .....                  | 7-33 |
| 7.3.1.2   | Preserving Application Metadata .....  | 7-33 |
| 7.3.1.3   | Preserving Portlet Customizations and Personalizations .....                 | 7-33 |
| 7.3.2     | Redeploying WebCenter Applications Using Fusion Middleware Control .....     | 7-33 |
| 7.3.3     | Redeploying WebCenter Applications Using WLST .....                          | 7-37 |

## 8 Starting and Stopping WebCenter Applications

|       |   |     |
|-------|---|-----|
| 8.1   | Starting Node Manager.....  | 8-1 |
| 8.2   | Starting and Stopping Managed Servers for WebCenter Application Deployments ..... | 8-2 |
| 8.3   | Starting and Stopping WebCenter Spaces.....                                       | 8-3 |
| 8.3.1 | Starting WebCenter Spaces Using Fusion Middleware Control .....                   | 8-4 |
| 8.3.2 | Starting WebCenter Spaces Using WLST.....   | 8-4 |
| 8.3.3 | Stopping WebCenter Spaces Using Fusion Middleware Control .....                   | 8-4 |
| 8.3.4 | Stopping WebCenter Spaces Using WLST.....   | 8-5 |
| 8.4   | Starting and Stopping Custom WebCenter Applications .....                         | 8-5 |
| 8.4.1 | Starting Custom WebCenter Applications Using Fusion Middleware Control.....       | 8-5 |
| 8.4.2 | Starting Custom WebCenter Applications Using WLST .....                           | 8-5 |
| 8.4.3 | Stopping Custom WebCenter Applications Using Fusion Middleware Control.....       | 8-6 |
| 8.4.4 | Stopping Custom WebCenter Applications Using WLST .....                           | 8-6 |

## 9 Setting Application Properties

|       |  |     |
|-------|--|-----|
| 9.1   | Setting Application Properties for WebCenter Spaces.....             | 9-1 |
| 9.1.1 | Specifying the BPEL Server Hosting WebCenter Spaces Workflows .....  | 9-1 |
| 9.2   | Setting Additional Properties for Custom WebCenter Applications..... | 9-2 |

## 10 Managing Content Repositories

|      |   |      |
|------|---|------|
| 10.1 | What You Should Know About Content Repository Connections ..... | 10-2 |
|------|---|------|

|            |  |       |
|------------|--|-------|
| 10.2       | Content Repository Prerequisites .....   | 10-3  |
| 10.2.1     | Oracle Content Server Prerequisites .....  | 10-3  |
| 10.2.1.1   | Oracle Content Server - Installation.....  | 10-3  |
| 10.2.1.2   | Oracle Content Server - Configuration.....   | 10-3  |
| 10.2.1.2.1 | Configuring the Identity Store .....   | 10-3  |
| 10.2.1.2.2 | Enabling Full-Text Searching and Indexing.....   | 10-5  |
| 10.2.1.2.3 | Configuring Secure Socket Layer (SSL) .....  | 10-5  |
| 10.2.1.3   | Oracle Content Server - Security Considerations .....  | 10-8  |
| 10.2.1.4   | Oracle Content Server - Limitations in WebCenter .....   | 10-8  |
| 10.2.2     | Oracle Portal Prerequisites .....  | 10-9  |
| 10.2.2.1   | Oracle Portal - Installation.....  | 10-9  |
| 10.2.2.2   | Oracle Portal - Configuration .....  | 10-9  |
| 10.2.2.3   | Oracle Portal - Security Considerations .....  | 10-9  |
| 10.2.2.4   | Oracle Portal - Limitations in WebCenter.....  | 10-9  |
| 10.2.3     | File System Prerequisites .....  | 10-10 |
| 10.2.3.1   | File System - Security Considerations .....  | 10-10 |
| 10.2.3.2   | File System - Limitations in WebCenter.....  | 10-10 |
| 10.3       | Registering Content Repositories .....   | 10-10 |
| 10.3.1     | Registering Content Repositories Using Fusion Middleware Control .....                                       | 10-10 |
| 10.3.2     | Registering Content Repositories Using WLST .....  | 10-15 |
| 10.4       | Changing the Active (or Default) Content Repository Connection .....   | 10-16 |
| 10.4.1     | Changing the Active (or Default) Content Repository Connection Using Fusion<br>Middleware Control            | 10-16 |
| 10.4.2     | Changing the Active (or Default) Content Repository Connection Using WLST.                                   | 10-17 |
| 10.5       | Modifying Content Repository Connection Details .....  | 10-17 |
| 10.5.1     | Modifying Content Repository Connection Details Using Fusion Middleware Control .<br>10-17                   |       |
| 10.5.2     | Modifying Content Repository Connection Details Using WLST.....  | 10-18 |
| 10.6       | Deleting Content Repository Connections.....   | 10-18 |
| 10.6.1     | Deleting Content Repository Connections Using Fusion Middleware Control....                                  | 10-18 |
| 10.6.2     | Deleting Content Repository Connections Using WLST .....   | 10-19 |
| 10.7       | Setting Connection Properties for the WebCenter Spaces Content Repository.....                               | 10-19 |
| 10.7.1     | Setting Connection Properties for the WebCenter Spaces Content Repository Using<br>Fusion Middleware Control | 10-19 |
| 10.7.2     | Setting Connection Properties for the WebCenter Spaces Content Repository Using<br>WLST                      | 10-20 |
| 10.8       | Testing Content Repository Connections.....  | 10-21 |
| 10.8.1     | Testing Oracle Content Server Connections .....  | 10-21 |
| 10.8.2     | Testing Oracle Portal Connections .....  | 10-22 |
| 10.9       | Changing the Maximum File Upload Size .....  | 10-24 |

## 11 Managing Services

|          |  |      |
|----------|--|------|
| 11.1     | Setting Up Connections for the Discussions and Announcements Services..... | 11-2 |
| 11.1.1   | What You Should Know About Discussion Server Connections .....             | 11-2 |
| 11.1.2   | Discussion Server Prerequisites.....                                       | 11-2 |
| 11.1.2.1 | Discussion Server - Installation .....                                     | 11-3 |
| 11.1.2.2 | Discussion Server - Configuration .....                                    | 11-3 |
| 11.1.2.3 | Discussion Server - Security Considerations.....                           | 11-3 |

|            |   |       |
|------------|---|-------|
| 11.1.2.4   | Discussion Server - Limitations.....  | 11-3  |
| 11.1.3     | Registering Discussion Servers.....   | 11-4  |
| 11.1.3.1   | Registering Discussion Servers Using Fusion Middleware Control.....                               | 11-4  |
| 11.1.3.2   | Registering Discussion Servers Using WLST .....   | 11-7  |
| 11.1.4     | Choosing the Active Connection for Discussions and Announcements.....                             | 11-7  |
| 11.1.4.1   | Choosing the Active Connection for Discussions and Announcements Using Fusion Middleware Control  | 11-8  |
| 11.1.4.2   | Choosing the Active Discussion for Discussions and Announcements Using WLST                       | 11-8  |
| 11.1.5     | Modifying Discussion Server Connection Details .....  | 11-9  |
| 11.1.5.1   | Modifying Discussion Server Connection Details Using Fusion Middleware Control                    | 11-9  |
| 11.1.5.2   | Modifying Discussion Server Connection Details Using WLST .....                                   | 11-9  |
| 11.1.6     | Deleting Discussion Server Connections.....   | 11-10 |
| 11.1.6.1   | Deleting a Discussion Server Connection Using Fusion Middleware Control .....                     | 11-10 |
| 11.1.6.2   | Deleting a Discussion Server Connection Using WLST.....   | 11-11 |
| 11.1.7     | Setting Up Discussions Service Defaults.....  | 11-11 |
| 11.1.8     | Setting Up Announcements Service Defaults.....  | 11-12 |
| 11.1.9     | Testing Discussion Server Connections.....  | 11-12 |
| 11.2       | Setting Up Connections for the Instant Messaging and Presence Service.....                        | 11-12 |
| 11.2.1     | What You Should Know About Instant Messaging and Presence Connections ...                         | 11-12 |
| 11.2.2     | Instant Messaging and Presence Server Prerequisites .....   | 11-13 |
| 11.2.2.1   | Oracle WebLogic Communications Server (OWLCS) Prerequisites.....                                  | 11-13 |
| 11.2.2.1.1 | OWLCS - Installation .....  | 11-13 |
| 11.2.2.1.2 | OWLCS - Configuration.....  | 11-13 |
| 11.2.2.1.3 | OWLCS - Security Considerations.....  | 11-13 |
| 11.2.2.1.4 | OWLCS - Limitations.....  | 11-14 |
| 11.2.2.2   | Microsoft Live Communications Server (LCS) Prerequisites .....                                    | 11-14 |
| 11.2.2.2.1 | LCS - Installation .....  | 11-14 |
| 11.2.2.2.2 | LCS - Configuration .....   | 11-14 |
| 11.2.2.2.3 | LCS - Security Considerations.....  | 11-17 |
| 11.2.2.2.4 | LCS - Limitations.....  | 11-17 |
| 11.2.3     | Registering Instant Messaging and Presence Servers .....  | 11-18 |
| 11.2.3.1   | Registering Instant Messaging and Presence Servers Using Fusion Middleware Control                | 11-18 |
| 11.2.3.2   | Registering Instant Messaging and Presence Servers Using WLST.....                                | 11-22 |
| 11.2.4     | Choosing the Active Connection for Instant Messaging and Presence .....                           | 11-22 |
| 11.2.4.1   | Choosing the Active Connection for Instant Messaging and Presence Using Fusion Middleware Control | 11-23 |
| 11.2.4.2   | Choosing the Active Connection for Instant Messaging and Presence Using WLST                      | 11-23 |
| 11.2.5     | Modifying Instant Messaging and Presence Connection Details .....                                 | 11-24 |
| 11.2.5.1   | Modifying Instant Messaging and Presence Connections Details Using Fusion Middleware Control      | 11-24 |
| 11.2.5.2   | Modifying Instant Messaging and Presence Connections Details Using WLST.....                      | 11-24 |
| 11.2.6     | Deleting Instant Messaging and Presence Connections .....   | 11-25 |

|          |  |       |
|----------|--|-------|
| 11.2.6.1 | Deleting Instant Messaging and Presence Connections Using Fusion Middleware Control                  | 11-25 |
| 11.2.6.2 | Deleting Instant Messaging and Presence Connections Using WLST.....                                  | 11-26 |
| 11.2.7   | Setting Up Instant Messaging and Presence Service Defaults .....                                     | 11-26 |
| 11.2.8   | Testing Instant Messaging and Presence Connections .....   | 11-26 |
| 11.3     | Setting Up Connections for the Mail Service .....  | 11-26 |
| 11.3.1   | What You Should Know About Mail Server Connections .....   | 11-27 |
| 11.3.2   | Mail Server Prerequisites.....   | 11-27 |
| 11.3.2.1 | Mail Server - Installation .....   | 11-27 |
| 11.3.2.2 | Mail Server - Configuration .....  | 11-27 |
| 11.3.2.3 | Mail Server - Security Considerations.....   | 11-28 |
| 11.3.2.4 | Mail Server - Limitations.....   | 11-28 |
| 11.3.3   | Registering Mail Servers .....   | 11-28 |
| 11.3.3.1 | Registering Mail Servers Using Fusion Middleware Control.....  | 11-28 |
| 11.3.3.2 | Registering Mail Servers Using WLST .....  | 11-32 |
| 11.3.4   | Choosing the Active (or Default) Mail Server Connection.....   | 11-32 |
| 11.3.4.1 | Choosing the Active (or Default) Mail Server Connection Using Fusion Middleware Control              | 11-33 |
| 11.3.4.2 | Choosing the Active (or Default) Mail Server Connection Using WLST .....                             | 11-33 |
| 11.3.5   | Modifying Mail Server Connection Details .....   | 11-34 |
| 11.3.5.1 | Modifying Mail Server Connection Details Using Fusion Middleware Control .....                       | 11-34 |
| 11.3.5.2 | Modifying Mail Server Connection Details Using WLST.....   | 11-34 |
| 11.3.6   | Deleting Mail Server Connections.....  | 11-35 |
| 11.3.6.1 | Deleting a Mail Connection Using Fusion Middleware Control.....                                      | 11-35 |
| 11.3.6.2 | Deleting a Mail Connection Using WLST.....   | 11-35 |
| 11.3.7   | Setting Up Mail Service Defaults.....  | 11-36 |
| 11.3.8   | Testing Mail Server Connections.....   | 11-36 |
| 11.4     | Setting Up Connections for the Search Service.....   | 11-36 |
| 11.4.1   | What You Should Know About Oracle Secure Enterprise Search Connections ...                           | 11-36 |
| 11.4.2   | Oracle Secure Enterprise Search Prerequisites .....  | 11-36 |
| 11.4.2.1 | Oracle Secure Enterprise Search - Installation .....   | 11-37 |
| 11.4.2.2 | Oracle Secure Enterprise Search - Configuration .....  | 11-37 |
| 11.4.2.3 | Oracle Secure Enterprise Search - Security .....   | 11-37 |
| 11.4.2.4 | Oracle Secure Enterprise Search - Limitations .....  | 11-37 |
| 11.4.3   | Registering Oracle Secure Enterprise Search Services .....   | 11-37 |
| 11.4.3.1 | Registering SES Search Services Using Fusion Middleware Control .....                                | 11-37 |
| 11.4.3.2 | Registering SES Services Using WLST .....  | 11-40 |
| 11.4.4   | Choosing the Active Oracle Secure Enterprise Search Connection.....                                  | 11-40 |
| 11.4.4.1 | Choosing the Active Oracle Secure Enterprise Search (SES) Connection Using Fusion Middleware Control | 11-40 |
| 11.4.4.2 | Choosing the Active Oracle Secure Enterprise Search (SES) Connection Using WLST                      | 11-41 |
| 11.4.5   | Modifying Oracle Secure Enterprise Search (SES) Connection Details .....                             | 11-41 |
| 11.4.5.1 | Modifying Oracle Secure Enterprise Search (SES) Connection Details Using Fusion Middleware Control   | 11-41 |
| 11.4.5.2 | Modifying Search Service Properties Using WLST .....   | 11-42 |
| 11.4.5.3 | Modifying SES Connection Details Using WLST .....  | 11-42 |

|            |   |       |
|------------|---|-------|
| 11.4.6     | Deleting Oracle Secure Enterprise Search (SES) Connections .....            | 11-42 |
| 11.4.6.1   | Deleting Search Connections Using Fusion Middleware Control .....           | 11-43 |
| 11.4.6.2   | Deleting Search Connections Using WLST.....                                 | 11-43 |
| 11.4.7     | Testing Oracle Secure Enterprise Search (SES) Connections.....              | 11-43 |
| 11.5       | Setting Up Connections for the Worklist Service .....                       | 11-43 |
| 11.5.1     | BPEL Server Prerequisites .....   | 11-44 |
| 11.5.1.1   | BPEL Server - Installation and Configuration.....                           | 11-44 |
| 11.5.1.2   | BPEL Server - Security Considerations .....                                 | 11-44 |
| 11.5.1.3   | BPEL Server - Limitations .....   | 11-45 |
| 11.5.2     | Setting Up Worklist Connections .....                                       | 11-45 |
| 11.5.2.1   | What You Should Know About Worklist Connections .....                       | 11-45 |
| 11.5.2.2   | Registering Worklist Connections.....                                       | 11-45 |
| 11.5.2.2.1 | Registering Worklist Connections Using Fusion Middleware Control ...        | 11-46 |
| 11.5.2.2.2 | Registering Worklist Connections Using WLST.....                            | 11-48 |
| 11.5.2.3   | Activating a Worklist Connection.....                                       | 11-48 |
| 11.5.2.3.1 | Activating a Worklist Connections Using Fusion Middleware Control..         | 11-48 |
| 11.5.2.3.2 | Activating a Worklist Connections Using WLST .....                          | 11-49 |
| 11.5.2.4   | Modifying Worklist Connection Details .....                                 | 11-49 |
| 11.5.2.4.1 | Modifying Worklist Connection Details Using Fusion Middleware Control ..... | 11-50 |
| 11.5.2.4.2 | Modifying Worklist Connection Details Using WLST .....                      | 11-50 |
| 11.5.2.5   | Deleting Worklist Connections.....  | 11-50 |
| 11.5.2.5.1 | Deleting Worklist Connections Using Fusion Middleware Control.....          | 11-50 |
| 11.5.2.5.2 | Deleting Worklist Connections Using WLST .....                              | 11-51 |
| 11.5.2.6   | Testing Worklist Connections.....   | 11-51 |
| 11.6       | Setting Up the WebCenter Repository .....                                   | 11-51 |
| 11.7       | Setting Up the MDS Repository .....   | 11-53 |
| 11.8       | Setting Up the Server for Wiki and Blog Services.....                       | 11-53 |
| 11.8.1     | What You Should Know About the Wiki and Blog Server Interface .....         | 11-54 |
| 11.8.1.1   | About the General Menu .....  | 11-55 |
| 11.8.1.2   | About the Administration Mode.....  | 11-55 |
| 11.8.2     | Accessing Oracle WebCenter Wiki and Blog Server .....                       | 11-58 |
| 11.8.3     | Setting Up Domains and Menus .....  | 11-58 |
| 11.8.3.1   | Adding a Domain .....   | 11-59 |
| 11.8.3.2   | Editing a Domain Menu .....   | 11-60 |
| 11.8.3.3   | Managing Domain Members .....   | 11-62 |
| 11.8.3.4   | Managing Blog Authors .....   | 11-63 |
| 11.8.4     | Changing the Theme .....  | 11-64 |
| 11.8.5     | Creating a User Interface Template .....                                    | 11-64 |
| 11.8.6     | Unlocking a Page .....  | 11-65 |
| 11.8.7     | Setting Up Server Security.....   | 11-66 |
| 11.8.8     | Managing Users and Roles.....   | 11-66 |
| 11.8.8.1   | Managing Users .....  | 11-66 |
| 11.8.8.2   | Managing Permissions for a Role.....  | 11-67 |
| 11.8.9     | Enabling Anonymous Access .....   | 11-68 |
| 11.8.10    | Blocking an IP Address.....   | 11-69 |
| 11.8.11    | Deleting Wiki Pages and Blog Entries .....                                  | 11-69 |

|           |   |       |
|-----------|---|-------|
| 11.8.11.1 | Deleting a Wiki Page.....                                       | 11-69 |
| 11.8.11.2 | Deleting a Blog Entry .....                                     | 11-70 |
| 11.8.12   | Specifying Configuration Parameters.....                        | 11-70 |
| 11.8.13   | Configuring Wiki Repository.....                                | 11-71 |
| 11.8.14   | Specifying Features Supported on the Wiki and Blog Server ..... | 11-72 |
| 11.8.15   | Monitoring Oracle WebCenter Wiki and Blog Server.....           | 11-72 |
| 11.8.16   | Backing Up and Restoring Wiki Content.....                      | 11-73 |
| 11.9      | Setting Up the RSS Service .....                                | 11-73 |

## 12 Managing Portlet Producers

|        |   |       |
|--------|---|-------|
| 12.1   | What You Should Know About Portlet Producers .....  | 12-1  |
| 12.2   | Registering WSRP Producers .....  | 12-2  |
| 12.2.1 | Registering a WSRP Producer Using Fusion Middleware Control.....                            | 12-2  |
| 12.2.2 | Registering a WSRP Producer Using WLST .....  | 12-7  |
| 12.3   | Testing WSRP Producer Connections.....  | 12-7  |
| 12.4   | Registering Oracle PDK-Java Producers .....   | 12-8  |
| 12.4.1 | Registering an Oracle PDK-Java Producer Using Fusion Middleware Control.....                | 12-8  |
| 12.4.2 | Registering an Oracle PDK-Java Producer Using WLST .....                                    | 12-10 |
| 12.5   | Testing Oracle PDK-Java Producer Connections .....  | 12-11 |
| 12.6   | Editing Producer Registration Details .....   | 12-11 |
| 12.6.1 | Editing Producer Registration Details Using Fusion Middleware Control .....                 | 12-11 |
| 12.6.2 | Editing Producer Registration Details Using WLST .....                                      | 12-12 |
| 12.7   | Deregistering Producers .....   | 12-12 |
| 12.7.1 | Deregistering Producers Using Fusion Middleware Control .....                               | 12-13 |
| 12.7.2 | Deregister Producers Using WLST .....   | 12-13 |
| 12.8   | Deploying Portlet Producer Applications.....  | 12-13 |
| 12.8.1 | Understanding Portlet Producer Application Deployment .....                                 | 12-14 |
| 12.8.2 | Converting a JSR 168 Portlet Producer EAR File into a WSRP EAR File .....                   | 12-14 |
| 12.8.3 | Deploying Portlet Producer Applications Using Oracle JDeveloper.....                        | 12-15 |
| 12.8.4 | Deploying Portlet Producer Applications Using Fusion Middleware Control.....                | 12-15 |
| 12.8.5 | Deploying Portlet Producer Applications Using Oracle WebLogic Server Administration Console | 12-15 |
| 12.8.6 | Deploying Portlet Applications Using WLST .....   | 12-15 |

## 13 Managing External Applications

|        |   |      |
|--------|---|------|
| 13.1   | What You Should Know About External Applications .....                        | 13-1 |
| 13.2   | Registering External Applications.....  | 13-2 |
| 13.2.1 | Registering External Applications Using Fusion Middleware Control.....        | 13-3 |
| 13.2.2 | Registering External Applications Using WLST .....                            | 13-7 |
| 13.3   | Modifying External Application Connection Details .....                       | 13-7 |
| 13.3.1 | Modifying External Application Connection Using Fusion Middleware Control .   | 13-8 |
| 13.3.2 | Modifying External Application Connection Using WLST .....                    | 13-8 |
| 13.4   | Deleting External Application Connections.....                                | 13-8 |
| 13.4.1 | Deleting External Application Connections Using Fusion Middleware Control ... | 13-9 |
| 13.4.2 | Deleting External Application Connections Using WLST .....                    | 13-9 |

## Part IV Advanced Systems Administration for Oracle WebCenter

## 14 Managing Security

|          |   |       |
|----------|---|-------|
| 14.1     | Introduction to WebCenter Application Security .....                                      | 14-1  |
| 14.2     | Default Security Configuration.....   | 14-4  |
| 14.2.1   | Administrator Accounts .....  | 14-4  |
| 14.2.2   | Application Roles and Enterprise Roles in WebCenter Spaces .....                          | 14-4  |
| 14.2.3   | Default Identity and Policy Stores.....   | 14-5  |
| 14.2.3.1 | File-based Credential Store .....   | 14-5  |
| 14.2.4   | Default Policy Store Permissions and Grants .....   | 14-6  |
| 14.2.4.1 | Permission-based Authorization.....   | 14-6  |
| 14.2.4.2 | Role-mapping Based Authorization .....  | 14-6  |
| 14.2.4.3 | Default Policy Store Permissions for WebCenter Spaces .....                               | 14-6  |
| 14.2.4.4 | Default Code-based Grants.....  | 14-9  |
| 14.2.5   | Post-deployment Security Configuration Tasks .....  | 14-9  |
| 14.3     | Configuring the Identity Store .....  | 14-10 |
| 14.3.1   | Reassociating the Identity Store with an External LDAP .....                              | 14-11 |
| 14.3.2   | Tuning the Identity Store for Performance .....   | 14-17 |
| 14.3.3   | Adding Users to the Identity Store .....  | 14-18 |
| 14.3.3.1 | Adding Users Using the WLS Administration Console .....                                   | 14-18 |
| 14.3.3.2 | Adding Users to the Embedded LDAP Using an LDIF File .....                                | 14-22 |
| 14.3.4   | Moving the Administrator Account to an External LDAP Server .....                         | 14-26 |
| 14.3.5   | Granting the WebCenter Administrator Role to a WebCenter Spaces User.....                 | 14-31 |
| 14.3.5.1 | Granting the WebCenter Spaces Administrator Role Using Fusion Middleware Control 14-31    |       |
| 14.3.5.2 | Granting the WebCenter Spaces Administrator Role Using WLST.....                          | 14-34 |
| 14.3.6   | Configuring the Discussions Server to Share the Identity Store LDAP Server .....          | 14-35 |
| 14.3.7   | Configuring the Discussions Server to Share the Identity Store Embedded LDAP Server 14-36 |       |
| 14.3.8   | Configuring the Oracle Content Server to Share the Identity Store LDAP Server             | 14-37 |
| 14.4     | Configuring the Policy and Credential Store to Use OID.....                               | 14-37 |
| 14.4.1   | Creating a root Node.....   | 14-37 |
| 14.4.2   | Reassociating the Credential and Policy Store Using Fusion Middleware Control .....       | 14-38 |
| 14.4.3   | Reassociating the Credential and Policy Store Using WLST.....                             | 14-40 |
| 14.5     | Managing Users and Roles .....  | 14-41 |
| 14.6     | Configuring WebCenter Applications and Components to Use SSL.....                         | 14-42 |
| 14.6.1   | Securing the Browser Connection to WebCenter Spaces with SSL .....                        | 14-42 |
| 14.6.1.1 | Creating the Custom Keystore .....  | 14-42 |
| 14.6.1.2 | Configuring the Identity and Trust Keystores .....  | 14-44 |
| 14.6.1.3 | Configuring the SSL Connection.....   | 14-47 |
| 14.6.2   | Securing the Browser Connection to a Custom WebCenter Application with SSL.....           | 14-50 |
| 14.6.3   | Securing the Connection from Oracle HTTP Server to WebCenter Spaces with SSL .....        | 14-50 |
| 14.6.4   | Securing the Browser Connection to the Wiki Service with SSL.....                         | 14-54 |
| 14.6.5   | Securing the WebCenter Spaces Connection to Portlet Producers with SSL.....               | 14-60 |
| 14.6.6   | Securing the WebCenter Spaces Connection to the LDAP Identity Store.....                  | 14-68 |
| 14.6.6.1 | Exporting the OID Certificate Authority (CA).....   | 14-69 |

|            |   |        |
|------------|---|--------|
| 14.6.6.2   | Setting Up the WebLogic Server .....  | 14-69  |
| 14.6.7     | Securing the WebCenter Spaces Connection to OCS with SSL.....                               | 14-69  |
| 14.6.8     | Securing the WebCenter Spaces Connection to IMAP and SMTP with SSL.....                     | 14-69  |
| 14.6.9     | Securing the WebCenter Spaces Connection to Oracle SES with SSL .....                       | 14-70  |
| 14.6.10    | Securing the WebCenter Spaces Connection to OWLCS with SSL .....                            | 14-70  |
| 14.6.11    | Securing the WebCenter Spaces Connection to Microsoft Live Communication Server<br>with SSL | 14-71  |
| 14.7       | Configuring a WebCenter Application to Use Single Sign-On.....                              | 14-72  |
| 14.7.1     | Configuring Oracle Access Manager (OAM) .....   | 14-72  |
| 14.7.1.1   | OAM Components and Topology.....  | 14-73  |
| 14.7.1.2   | Configuring OAM Using Scripts.....  | 14-74  |
| 14.7.1.3   | Configuring the Webtier Components.....   | 14-76  |
| 14.7.1.3.1 | Configure mod_weblogic (mod_wl_ohs.conf).....   | 14-76  |
| 14.7.1.3.2 | Create an AccessGate Entry .....  | 14-76  |
| 14.7.1.3.3 | Install WebGate on the WebTier .....  | 14-78  |
| 14.7.1.4   | Manually Configuring the Access System.....   | 14-78  |
| 14.7.1.5   | Manually Defining the WebCenter Policy Domain.....  | 14-79  |
| 14.7.1.6   | Configuring the Policy Manager .....  | 14-85  |
| 14.7.1.6.1 | Configuring the Oracle Internet Directory Authenticator .....                               | 14-85  |
| 14.7.1.6.2 | Configuring the OAM Identity Asserter.....  | 14-90  |
| 14.7.1.6.3 | Configuring the Default Authenticator and Setting the Provider Order.                       | 14-93  |
| 14.7.1.6.4 | Configuring the Application for Oracle Access Manager SSO.....                              | 14-94  |
| 14.7.1.7   | Additional Configurations .....   | 14-94  |
| 14.7.1.7.1 | Configuring the WLS Administration Console and Enterprise Manager .....                     | 14-95  |
| 14.7.1.7.2 | Deploying the Discussions Server .....  | 14-97  |
| 14.7.1.7.3 | Configuring the Discussions Server .....  | 14-98  |
| 14.7.1.7.4 | Configuring the Wiki Server.....  | 14-98  |
| 14.7.1.7.5 | Restricting Access with Connection Filters .....  | 14-99  |
| 14.7.2     | Configuring Oracle Single Sign-On (OSSO) .....  | 14-100 |
| 14.7.2.1   | OSSO Components and Topology .....  | 14-101 |
| 14.7.2.2   | Configuring the Oracle HTTP Server and Associated mods .....                                | 14-101 |
| 14.7.2.3   | Configuring the OSSOIdentityAsserter .....  | 14-102 |
| 14.7.2.4   | Registering OHS with Oracle SSO .....   | 14-105 |
| 14.7.3     | Configuring SAML-based Single Sign-on.....  | 14-107 |
| 14.7.3.1   | SAML Components and Topology .....  | 14-107 |
| 14.7.3.2   | Configuring SAML-based Single Sign-on.....  | 14-110 |
| 14.7.3.2.1 | Checking the Default WebCenter Spaces and Services Login.....                               | 14-110 |
| 14.7.3.2.2 | Generating and Registering Certificates .....   | 14-111 |
| 14.7.3.2.3 | Creating the SAML Credential Mapping Provider Instance .....                                | 14-114 |
| 14.7.3.2.4 | Configuring a Relying Party .....   | 14-119 |
| 14.7.3.2.5 | Configuring Source Site Federation Services .....   | 14-128 |
| 14.7.3.2.6 | Configuring the SAML Identity Assertion Provider.....                                       | 14-130 |
| 14.7.3.2.7 | Configuring Destination Site Federation Services.....                                       | 14-149 |
| 14.7.3.2.8 | Checking Your Configuration .....   | 14-154 |
| 14.7.3.2.9 | Configuring the Discussions Server for SAML SSO .....                                       | 14-154 |
| 14.7.4     | Configuring SSO with Microsoft Clients.....   | 14-155 |
| 14.7.4.1   | Microsoft Client SSO Concepts.....  | 14-155 |



|            |  |        |
|------------|--|--------|
| 14.7.4.2   | System Requirements.....   | 14-157 |
| 14.7.4.3   | Configuring SSO with Microsoft Clients .....   | 14-158 |
| 14.7.4.3.1 | Configuring the Negotiate Identity Assertion Provider.....                                     | 14-159 |
| 14.7.4.3.2 | Configuring an Active Directory Authentication Provider .....                                  | 14-161 |
| 14.7.4.3.3 | Configuring WebCenter Spaces .....   | 14-167 |
| 14.8       | Configuring WS-Security.....   | 14-168 |
| 14.8.1     | Securing the BPEL Server with WS-Security .....  | 14-168 |
| 14.8.1.1   | Generating the Keystores .....   | 14-168 |
| 14.8.1.1.1 | Generating the Keystores in the WebCenter Spaces Keystore .....                                | 14-168 |
| 14.8.1.1.2 | Importing the Trusted Certificate of the WebCenter Spaces Keystore to the SOA Keystore         | 14-169 |
| 14.8.1.1.3 | Generating a Key Pair in the SOA Instance.....   | 14-169 |
| 14.8.1.1.4 | Exporting the Public Key of the SOA Instance .....   | 14-170 |
| 14.8.1.1.5 | Importing the Trusted Certificate of the SOA Instance in the WebCenter Instance                | 14-170 |
| 14.8.1.2   | Generating the Keystores When the SOA Server and WebCenter Share the Same Domain               | 14-171 |
| 14.8.1.3   | Registering the Keystores.....   | 14-172 |
| 14.8.1.3.1 | Registering the Keystores in the WebCenter Spaces Instance .....                               | 14-172 |
| 14.8.1.3.2 | Registering the Keystores in the SOA Instance.....   | 14-173 |
| 14.8.1.4   | Updating the Credential Stores .....   | 14-173 |
| 14.8.1.4.1 | Updating the Credential Store in the WebCenter Spaces Instance Using WLST                      | 14-173 |
| 14.8.1.4.2 | Updating the Credential Store in the WebCenter Spaces Instance Using Fusion Middleware Control | 14-174 |
| 14.8.1.4.3 | Updating the Credential Store in the SOA Instance Using WLST.....                              | 14-175 |
| 14.8.1.4.4 | Updating the Credential Store in the SOA Instance Using Fusion Middleware Control              | 14-175 |
| 14.8.2     | Securing the Discussions Server with WS-Security .....   | 14-176 |
| 14.8.2.1   | Creating the Keystore Certificate Properties File.....   | 14-176 |
| 14.8.2.2   | Specifying the Properties File for ClassLoader .....   | 14-177 |
| 14.8.2.3   | Updating the System Properties for WS-Security.....  | 14-178 |
| 14.8.3     | Securing Oracle WebLogic Communication Services (OWLCS) with WS-Security .....                 | 14-178 |
| 14.8.4     | Securing a WSRP Producer with WS-Security .....  | 14-180 |
| 14.8.4.1   | Deploying the Producer .....   | 14-180 |
| 14.8.4.2   | Attaching a Policy to the Producer Endpoint.....   | 14-181 |
| 14.8.4.3   | Setting Up the Keystores .....   | 14-185 |
| 14.8.4.3.1 | Creating the Keystores.....  | 14-185 |
| 14.8.4.3.2 | Configuring the Keystores .....  | 14-188 |
| 14.8.4.3.3 | Unconfiguring a Keystore Provider .....  | 14-190 |
| 14.8.5     | Securing WebCenter Spaces for Applications Consuming Spaces Client APIs with WS-Security       | 14-191 |
| 14.8.5.1   | Generating the Keystores .....   | 14-191 |
| 14.8.5.2   | Providing the Keystores and Keystore Information to the Application Developer ...              | 14-194 |
| 14.8.5.3   | Registering the Keystores.....   | 14-194 |
| 14.8.5.4   | Updating the Credential Stores .....   | 14-196 |

|          |   |        |
|----------|---|--------|
| 14.9     | Securing a PDK-Java Producer .....                              | 14-197 |
| 14.9.1   | Defining a Shared Key as a Password Credential .....            | 14-198 |
| 14.9.1.1 | Defining a Shared Key Using Fusion Middleware Control .....     | 14-198 |
| 14.9.1.2 | Defining a Shared Key Using WLST.....                           | 14-199 |
| 14.9.2   | Granting the PDK-Java Code Access to the Credential Store ..... | 14-200 |
| 14.9.2.1 | Granting Access Using Fusion Middleware Control .....           | 14-200 |
| 14.9.2.2 | Granting Access Using WLST.....                                 | 14-202 |

## 15 Monitoring Oracle WebCenter Performance

|           |   |       |
|-----------|---|-------|
| 15.1      | Understanding WebCenter Performance Metrics.....                      | 15-1  |
| 15.1.1    | Overview of Metric Collection: Recent History and Since Startup ..... | 15-2  |
| 15.1.2    | Overview of Common Metrics .....                                      | 15-3  |
| 15.1.3    | Common Performance Issues and Actions .....                           | 15-7  |
| 15.1.4    | Overview of Service-Specific Metrics .....                            | 15-8  |
| 15.1.4.1  | Announcements Metrics.....  | 15-9  |
| 15.1.4.2  | BPEL Worklist Metrics.....  | 15-10 |
| 15.1.4.3  | Content Repository (Documents Service) Metrics.....                   | 15-10 |
| 15.1.4.4  | Discussions Metrics .....   | 15-15 |
| 15.1.4.5  | Group Space Events Metrics .....                                      | 15-17 |
| 15.1.4.6  | External Application Metrics .....                                    | 15-19 |
| 15.1.4.7  | Instant Messaging and Presence (IMP) Metrics .....                    | 15-21 |
| 15.1.4.8  | Import and Export Metrics.....  | 15-22 |
| 15.1.4.9  | List Metrics .....  | 15-22 |
| 15.1.4.10 | Mail Metrics.....   | 15-24 |
| 15.1.4.11 | Note Metrics .....  | 15-26 |
| 15.1.4.12 | Page Metrics .....  | 15-27 |
| 15.1.4.13 | Portlet Producer Metrics.....   | 15-28 |
| 15.1.4.14 | Portlet Metrics.....  | 15-30 |
| 15.1.4.15 | RSS News Feed Metrics .....   | 15-34 |
| 15.1.4.16 | Recent Activity Metrics.....  | 15-34 |
| 15.1.4.17 | Search Metrics .....  | 15-35 |
| 15.1.5    | Service-Specific Performance Issues and Actions.....                  | 15-36 |
| 15.1.5.1  | Announcements Service .....   | 15-37 |
| 15.1.5.2  | BPEL Worklist Service .....   | 15-37 |
| 15.1.5.3  | Content Repository (Documents) Service.....                           | 15-37 |
| 15.1.5.4  | Discussions Service .....   | 15-37 |
| 15.1.5.5  | External Applications Service.....                                    | 15-38 |
| 15.1.5.6  | Group Space Events Service.....                                       | 15-38 |
| 15.1.5.7  | Instant Messaging and Presence (IMP) Service .....                    | 15-38 |
| 15.1.5.8  | Import and Export.....  | 15-38 |
| 15.1.5.9  | Lists Service .....   | 15-38 |
| 15.1.5.10 | Mail Service .....  | 15-38 |
| 15.1.5.11 | Notes Service .....   | 15-39 |
| 15.1.5.12 | Page Service.....   | 15-39 |
| 15.1.5.13 | Portlets and Producers.....   | 15-39 |
| 15.1.5.14 | RSS News Feed Service.....  | 15-39 |
| 15.1.5.15 | Recent Activities Service.....  | 15-40 |

|           |  |       |
|-----------|--|-------|
| 15.1.5.16 | Search Service.....                            | 15-40 |
| 15.1.6    | Group Space Metrics .....                      | 15-40 |
| 15.2      | Viewing Performance Information.....           | 15-42 |
| 15.2.1    | Monitoring WebCenter Spaces .....              | 15-42 |
| 15.2.2    | Monitoring Custom WebCenter Applications ..... | 15-43 |
| 15.3      | Viewing and Configuring Log Information.....   | 15-44 |
| 15.3.1    | WebCenter Spaces Logs.....                     | 15-44 |
| 15.3.2    | Custom WebCenter Application Logs.....         | 15-45 |

## 16 Managing Export, Import, Backup, and Recovery of WebCenter

|           |   |       |
|-----------|---|-------|
| 16.1      | Exporting and Importing WebCenter Spaces for Data Migration.....                        | 16-1  |
| 16.1.1    | Understanding WebCenter Spaces Export and Import .....                                  | 16-2  |
| 16.1.2    | Prerequisites for WebCenter Spaces Export and Import .....                              | 16-6  |
| 16.1.3    | Migrating Back-end Components for an Entire WebCenter Spaces Application ...            | 16-6  |
| 16.1.3.1  | Exporting the LDAP Identity Store.....  | 16-7  |
| 16.1.3.2  | Importing the LDAP Identity Store .....   | 16-7  |
| 16.1.3.3  | Exporting and Importing the LDAP Credential Store .....                                 | 16-8  |
| 16.1.3.4  | Exporting and Importing the LDAP Policy Store.....                                      | 16-10 |
| 16.1.3.5  | Exporting Oracle WebCenter Discussions Server.....                                      | 16-12 |
| 16.1.3.6  | Importing Oracle WebCenter Discussions Server .....                                     | 16-12 |
| 16.1.3.7  | Exporting Oracle WebCenter Wiki Server.....   | 16-13 |
| 16.1.3.8  | Importing Oracle WebCenter Wiki Server .....  | 16-14 |
| 16.1.3.9  | Exporting Oracle Content Server .....   | 16-15 |
| 16.1.3.10 | Importing Oracle Content Server .....   | 16-15 |
| 16.1.3.11 | Exporting Oracle WebLogic Communications Server .....                                   | 16-16 |
| 16.1.3.12 | Importing Oracle WebLogic Communications Server.....                                    | 16-16 |
| 16.1.3.13 | Exporting Portlet Producers .....   | 16-16 |
| 16.1.3.14 | Importing Portlet Producers .....   | 16-17 |
| 16.1.4    | Exporting an Entire WebCenter Spaces Application.....                                   | 16-17 |
| 16.1.4.1  | Exporting WebCenter Spaces Using Oracle Enterprise Manager Fusion<br>Middleware Control | 16-17 |
| 16.1.4.2  | Exporting WebCenter Spaces Using WLST .....   | 16-20 |
| 16.1.5    | Importing an Entire WebCenter Spaces Application .....                                  | 16-20 |
| 16.1.5.1  | Importing WebCenter Spaces Using Oracle Enterprise Manager Fusion<br>Middleware Control | 16-21 |
| 16.1.5.2  | Importing WebCenter Spaces Using WLST.....  | 16-22 |
| 16.1.6    | Prerequisites for Group Space Export and Import .....                                   | 16-22 |
| 16.1.7    | Migrating Back-end Components for Individual Group Spaces .....                         | 16-22 |
| 16.1.7.1  | Exporting Discussions for a Group Space.....  | 16-23 |
| 16.1.7.2  | Importing Discussions for a Group Space .....   | 16-25 |
| 16.1.7.3  | Exporting Wikis and Blogs for a Group Space.....  | 16-27 |
| 16.1.7.4  | Importing Wikis and Blogs for a Group Space .....                                       | 16-28 |
| 16.1.7.5  | Exporting Documents for a Group Space .....   | 16-29 |
| 16.1.7.6  | Importing Documents for a Group Space.....  | 16-29 |
| 16.1.8    | Exporting Group Spaces .....  | 16-30 |
| 16.1.8.1  | Exporting Group Spaces Using WebCenter Spaces .....                                     | 16-31 |
| 16.1.8.2  | Exporting Group Spaces Using WLST .....   | 16-31 |

|           |  |       |
|-----------|--|-------|
| 16.1.9    | Importing Group Spaces.....  | 16-31 |
| 16.1.9.1  | Importing Group Spaces Using WebCenter Spaces .....  | 16-32 |
| 16.1.9.2  | Importing Group Spaces Using WLST.....   | 16-32 |
| 16.1.10   | Migrating Back-end Components for Group Space Templates .....                                | 16-32 |
| 16.1.11   | Exporting Group Space Templates .....  | 16-32 |
| 16.1.11.1 | Exporting Group Space Templates Using WebCenter Spaces.....                                  | 16-32 |
| 16.1.11.2 | Exporting Group Space Templates Using WLST.....  | 16-32 |
| 16.1.12   | Importing Group Space Templates.....   | 16-33 |
| 16.1.12.1 | Importing Group Space Templates Using WebCenter Spaces .....                                 | 16-33 |
| 16.1.12.2 | Importing Group Space Templates Using WLST .....   | 16-33 |
| 16.2      | Exporting and Importing Custom WebCenter Applications for Data Migration .....               | 16-33 |
| 16.2.1    | Understanding Custom WebCenter Application Export and Import .....                           | 16-34 |
| 16.2.2    | Prerequisites for Custom WebCenter Application Export and Import .....                       | 16-34 |
| 16.2.3    | Exporting Portlet Client Metadata (Custom WebCenter Applications).....                       | 16-35 |
| 16.2.4    | Importing Portlet Client Metadata (Custom WebCenter Applications).....                       | 16-35 |
| 16.2.5    | Exporting WebCenter Web 2.0 Services Metadata and Data (Custom WebCenter Applications) 16-36 |       |
| 16.2.6    | Importing WebCenter Web 2.0 Services Metadata and Data (Custom WebCenter Applications) 16-38 |       |
| 16.2.7    | Migrating Security for Custom WebCenter Applications .....                                   | 16-39 |
| 16.2.8    | Migrating Data (Custom WebCenter Applications).....  | 16-39 |
| 16.2.8.1  | Exporting Data (Custom WebCenter Applications).....  | 16-39 |
| 16.2.8.2  | Importing Data (Custom WebCenter Applications) .....   | 16-40 |
| 16.3      | Backing Up and Recovering WebCenter Applications .....                                       | 16-41 |

## Part V Application Administration for Oracle WebCenter Spaces

### 17 Accessing WebCenter Spaces Administration Pages

|      |   |      |
|------|---|------|
| 17.1 | Logging into WebCenter Spaces as an Administrator ..... | 17-1 |
| 17.2 | WebCenter Spaces Administration Pages .....             | 17-2 |

### 18 Customizing WebCenter Spaces

|        |   |       |
|--------|---|-------|
| 18.1   | Naming Your WebCenter .....   | 18-1  |
| 18.2   | Customizing the Online Help Link .....  | 18-2  |
| 18.3   | Customizing the Sidebar.....  | 18-3  |
| 18.3.1 | Hiding and Showing Task Flows in the Sidebar.....   | 18-4  |
| 18.3.2 | Locking Sidebar Content .....   | 18-4  |
| 18.4   | Changing the WebCenter Logo .....   | 18-5  |
| 18.5   | Applying Look and Feel using Skins .....  | 18-6  |
| 18.5.1 | What You Should Know About Application Skins .....  | 18-6  |
| 18.5.2 | Selecting a Skin.....   | 18-7  |
| 18.5.3 | Making New Skins Available to WebCenter Spaces .....                                      | 18-7  |
| 18.6   | Customizing Copyright and Privacy Statements.....   | 18-7  |
| 18.7   | Choosing the Default Display Language .....   | 18-8  |
| 18.8   | Setting Discussion Forum Options.....   | 18-10 |
| 18.8.1 | Specifying Where Discussions and Announcements are Stored on the Discussions Server 18-11 |       |

|        |   |       |
|--------|---|-------|
| 18.8.2 | Setting Up a Default Group Space Discussion Forum .....             | 18-12 |
| 18.8.3 | Enabling Discussion Forums to Publish Group Space Mail.....         | 18-12 |
| 18.9   | Managing Personal Profiles.....                                     | 18-13 |
| 18.10  | Enabling and Disabling WebCenter Services .....                     | 18-15 |
| 18.11  | Enabling and Disabling Personal Spaces.....                         | 18-17 |
| 18.12  | Publishing the WebDAV URL .....                                     | 18-17 |
| 18.13  | Overriding and Customizing Application Templates.....               | 18-18 |
| 18.14  | Making New Page Styles Available .....                              | 18-19 |
| 18.15  | Customizing the Resource Catalog and Deploying New Task Flows ..... | 18-20 |

## 19 Managing Users and Roles for WebCenter Spaces

|          |  |       |
|----------|--|-------|
| 19.1     | Understanding Users, Roles, and Permissions.....                   | 19-1  |
| 19.1.1   | Understanding Users .....  | 19-1  |
| 19.1.2   | Understanding Application Roles.....                               | 19-2  |
| 19.1.2.1 | Default Application Roles .....                                    | 19-2  |
| 19.1.2.2 | Custom Application Roles .....                                     | 19-3  |
| 19.1.3   | Understanding Application Permissions .....                        | 19-3  |
| 19.1.4   | Understanding Discussions Server Role and Permission Mapping ..... | 19-5  |
| 19.2     | Managing Users .....   | 19-6  |
| 19.2.1   | What You Need to Know About Managing Users .....                   | 19-6  |
| 19.2.2   | Assigning Users to Roles .....                                     | 19-7  |
| 19.2.3   | Assigning a User to a Different Role.....                          | 19-8  |
| 19.2.4   | Giving a User Administrative Privileges .....                      | 19-10 |
| 19.2.5   | Revoking Application Roles.....                                    | 19-10 |
| 19.2.6   | Adding or Removing Users.....                                      | 19-11 |
| 19.3     | Managing Application Roles and Permissions.....                    | 19-11 |
| 19.3.1   | What You Need to Know About Application Roles and Permissions..... | 19-12 |
| 19.3.2   | Defining Application Roles .....                                   | 19-12 |
| 19.3.3   | Modifying Application Role Permissions .....                       | 19-13 |
| 19.3.4   | Granting Permissions to the Public-User .....                      | 19-14 |
| 19.3.5   | Granting Permissions to the Spaces-User .....                      | 19-14 |
| 19.3.6   | Deleting Application Roles.....                                    | 19-15 |
| 19.4     | Allowing Self-Registration .....                                   | 19-16 |
| 19.4.1   | Enabling Self-Registration By Invitation-Only .....                | 19-16 |
| 19.4.2   | Enabling Anyone to Self-Register.....                              | 19-17 |

## 20 Managing Pages in WebCenter Spaces

|        |  |       |
|--------|--|-------|
| 20.1   | Managing Business Role Pages.....                              | 20-1  |
| 20.1.1 | What You Should Know About Business Role Pages .....           | 20-1  |
| 20.1.2 | Creating a Business Role Page .....                            | 20-2  |
| 20.1.3 | Specifying the Target Audience for Business Role Pages.....    | 20-3  |
| 20.1.4 | Choosing a Default Display Order for Business Role Pages ..... | 20-6  |
| 20.1.5 | Editing a Business Role Page .....                             | 20-7  |
| 20.1.6 | Copying a Business Role Page .....                             | 20-8  |
| 20.1.7 | Deleting a Business Role Page .....                            | 20-9  |
| 20.2   | Managing Personal Pages.....                                   | 20-10 |

|        |  |       |
|--------|--|-------|
| 20.2.1 | What You Should Know About Personal Page Management.....                     | 20-10 |
| 20.2.2 | Setting Up a Default Look and Feel for Personal Pages.....                   | 20-11 |
| 20.2.3 | Editing Personal Pages with Administrative Privileges .....                  | 20-12 |
| 20.2.4 | Changing Access Permissions for a Personal Page.....                         | 20-13 |
| 20.2.5 | Copying a Personal Page .....  | 20-15 |
| 20.2.6 | Deleting a Personal Page .....   | 20-16 |
| 20.3   | Setting Up the Public User Experience .....                                  | 20-17 |
| 20.3.1 | Customizing the Public Welcome Page.....                                     | 20-17 |
| 20.3.2 | Customizing the Login Page .....   | 20-18 |
| 20.3.3 | Customizing the Self-Registration Page .....                                 | 20-20 |
| 20.3.4 | Preventing Public Users Seeing Any Personal Page or Business Role Page ..... | 20-21 |

## 21 Making Applications Available in WebCenter Spaces

|      |   |      |
|------|---|------|
| 21.1 | What You Should Know About the Applications Pane .....        | 21-1 |
| 21.2 | Making an Application Available to WebCenter Users .....      | 21-2 |
| 21.3 | Editing Links in the Applications Pane .....                  | 21-5 |
| 21.4 | Arranging the Applications List .....                         | 21-6 |
| 21.5 | Locking Applications Displayed in the Applications Pane ..... | 21-7 |
| 21.6 | Removing Links from the Applications Pane .....               | 21-8 |

## 22 Managing Group Spaces in WebCenter Spaces

|        |  |      |
|--------|--|------|
| 22.1   | What You Should Know About Group Space Management.....         | 22-1 |
| 22.2   | Viewing Group Space Information .....                          | 22-2 |
| 22.3   | Changing the Status of a Group Space .....                     | 22-2 |
| 22.3.1 | Taking Any Group Space Offline .....                           | 22-3 |
| 22.3.2 | Bringing Any Group Space Back Online.....                      | 22-3 |
| 22.3.3 | Closing Any Group Space .....                                  | 22-4 |
| 22.3.4 | Reactivating Any Group Space.....                              | 22-5 |
| 22.3.5 | Deleting a Group Space .....                                   | 22-6 |
| 22.4   | Enabling and Disabling Services .....                          | 22-6 |
| 22.5   | Managing Group Space Templates .....                           | 22-7 |
| 22.5.1 | What You Should Know About Managing Group Space Templates..... | 22-7 |
| 22.5.2 | Viewing Group Space Templates .....                            | 22-7 |
| 22.5.3 | Deleting a Group Space Template.....                           | 22-8 |
| 22.6   | Publishing and Unpublishing Group Space Templates.....         | 22-9 |

## 23 Exporting and Importing Group Spaces

|      |                                       |      |
|------|---------------------------------------|------|
| 23.1 | Exporting Group Spaces .....          | 23-1 |
| 23.2 | Importing Group Spaces .....          | 23-4 |
| 23.3 | Exporting Group Space Templates.....  | 23-6 |
| 23.4 | Importing Group Space Templates ..... | 23-7 |

## Part VI Appendixes

### A WebCenter Configuration

|     |                           |     |
|-----|---------------------------|-----|
| A.1 | Configuration Files ..... | A-1 |
|-----|---------------------------|-----|

|        |   |      |
|--------|---|------|
| A.1.1  | adf-config.xml and connections.xml.....   | A-1  |
| A.1.2  | web.xml.....  | A-4  |
| A.2    | Cluster Configuration.....  | A-5  |
| A.3    | Configuration Tools.....  | A-5  |
| A.3.1  | Configuration Through Fusion Middleware Control, WLST Commands, and System MBeans Browser | A-5  |
| A.3.2  | Editing Configuration Files Manually.....   | A-6  |
| A.4    | Tuning Environment Configuration.....   | A-6  |
| A.4.1  | Setting System Limit.....   | A-6  |
| A.4.2  | Setting JDBC Data Source.....   | A-7  |
| A.4.3  | Setting JRockit Virtual Machine (JVM) Arguments.....                                      | A-7  |
| A.5    | Tuning WebCenter Application Configuration.....   | A-8  |
| A.5.1  | Setting HTTP Session Timeout.....   | A-8  |
| A.5.2  | Setting JSP Page Timeout.....   | A-9  |
| A.5.3  | Setting ADF Client State Token.....   | A-9  |
| A.5.4  | Setting MDS Cache Size and Purge Rate.....  | A-9  |
| A.5.5  | Configuring Concurrency Management.....   | A-10 |
| A.5.6  | Configuring CRUD APIs (Create, Read, Update and Delete).....                              | A-11 |
| A.6    | Tuning Back-End Component Configuration.....  | A-11 |
| A.6.1  | Tuning Performance of the Announcements Service.....                                      | A-12 |
| A.6.2  | Tuning Performance of the Discussions Service.....  | A-12 |
| A.6.3  | Tuning Performance of the IMP Service.....  | A-13 |
| A.6.4  | Tuning Performance of the Mail Service.....   | A-13 |
| A.6.5  | Tuning Performance of the RSS News Feed Service.....                                      | A-14 |
| A.6.6  | Tuning Performance of the Search Service.....   | A-14 |
| A.6.7  | Tuning Performance of WSRP Producers.....   | A-15 |
| A.6.8  | Tuning Performance of Oracle PDK-Java Producers.....                                      | A-15 |
| A.6.9  | Tuning Performance of OmniPortlet.....  | A-15 |
| A.6.10 | Tuning Performance of the Portlet Service.....  | A-16 |
| A.6.11 | Configuring Portlet Cache Size.....   | A-17 |
| A.6.12 | Configuring Portlet Timeout.....  | A-17 |

## **B Troubleshooting**

|       |  |     |
|-------|--|-----|
| B.1   | Troubleshooting WebCenter Application Configuration Issues.....                            | B-1 |
| B.1.1 | WebCenter Does Not Display in the Application Deployment Menu in Fusion Middleware Control | B-1 |
| B.1.2 | Configuration Options Unavailable.....   | B-3 |
| B.1.3 | Configuration Performed in One Application Reflects in Another.....                        | B-3 |
| B.2   | Troubleshooting WLST Command Issues.....   | B-4 |
| B.2.1 | None of the WLST Commands Work.....  | B-4 |
| B.2.2 | WLST Commands Do Not Work for a Particular Service.....                                    | B-4 |
| B.2.3 | A Connection with the Name Connection_Name Already Exists.....                             | B-5 |
| B.2.4 | WLST Shell is Not Connected to the Oracle WebLogic Managed Server Instance...              | B-6 |
| B.2.5 | Application with the Same Name Already Exists in a Domain.....                             | B-6 |
| B.2.6 | Application with the Same Name Already Exists on a Managed Server.....                     | B-6 |
| B.2.7 | Already in Domain Runtime Tree Message Displays.....                                       | B-7 |
| B.3   | Troubleshooting Discussions Service Issues.....  | B-7 |

|         |   |      |
|---------|---|------|
| B.3.1   | Discussion Forum Cannot Be Enabled in Group Spaces .....                          | B-7  |
| B.3.2   | Login Does Not Function Properly After Configuring OAM-SSO .....                  | B-8  |
| B.4     | Troubleshooting Instant Messaging and Presence Service Issues .....               | B-8  |
| B.5     | Troubleshooting Mail Service Issues.....  | B-9  |
| B.5.1   | Mail Service is Not Accessible in Secure Mode.....                                | B-9  |
| B.5.2   | Mail Service is Not Accessible in Non-Secure Mode.....                            | B-9  |
| B.5.3   | Unable to Create Distribution Lists in the Non-Secure Mode .....                  | B-9  |
| B.5.4   | Unable to Create Distribution Lists in the Secure Mode.....                       | B-10 |
| B.5.5   | Unable to Configure the Number of Mails Downloaded .....                          | B-10 |
| B.5.6   | Unable to Publish and Archive Group Space Mail.....                               | B-11 |
| B.6     | Troubleshooting Portlet Producer Issues .....                                     | B-11 |
| B.6.1   | Producer Registration Fails for a Custom WebCenter Application .....              | B-11 |
| B.6.2   | Portlet Unavailable: WSM-00101 Exception .....                                    | B-12 |
| B.7     | Troubleshooting Wiki and Blog Issues .....  | B-12 |
| B.8     | Troubleshooting Worklist Service Issues .....                                     | B-13 |
| B.8.1   | Unavailability of the Worklist Service Due to Application Configuration Issues .. | B-13 |
| B.8.1.1 | adf-config.xml Refers to a Non-Existent BPEL Connection .....                     | B-13 |
| B.8.1.2 | adf-config.xml Has No Reference to a BPEL Connection.....                         | B-14 |
| B.8.1.3 | No Rows Yet Message Displays .....  | B-14 |
| B.8.2   | Unavailability of the Worklist Service Due to Server Failure .....                | B-15 |
| B.8.2.1 | Users Mismatch in Identity Stores .....   | B-16 |
| B.8.2.2 | Shared User Directory Does Not Include the weblogic User.....                     | B-17 |
| B.8.2.3 | Issues with the wsm-pm Application.....   | B-18 |
| B.8.2.4 | Clocks are Out of Sync for More Than Five Minutes .....                           | B-18 |
| B.8.2.5 | Worklist Service Timed Out or is Disabled .....                                   | B-18 |
| B.9     | Troubleshooting WebCenter Spaces Import and Export Issues .....                   | B-19 |
| B.9.1   | ResourceLimitException Issue.....   | B-20 |
| B.9.2   | Page or Group Space Not Found Message After Import.....                           | B-20 |
| B.9.3   | Group Space Import Exceed Maximum Upload File Size .....                          | B-20 |

## Glossary

## Index



## List of Examples

|       |   |        |
|-------|---|--------|
| 10-1  | Sample Output Generated by the Keytool.....                   | 10-7   |
| 10-2  | Sample sslconfig.hda File.....                                | 10-8   |
| 14-1  | Import Trusted Certificate in the SOA Instance.....           | 14-169 |
| 14-2  | Generate a Key Pair In the SOA Instance.....                  | 14-170 |
| 14-3  | Export the Public Key of the SOA Instance.....                | 14-170 |
| 14-4  | Import the Trusted Certificate in the WebCenter Instance..... | 14-171 |
| 14-5  | .....   | 14-171 |
| 14-6  | .....   | 14-172 |
| 14-7  | .....   | 14-172 |
| 14-8  | keystore-csf-key.....   | 14-173 |
| 14-9  | enc-csf-key.....  | 14-174 |
| 14-10 | sign-csf-key.....   | 14-174 |
| 14-11 | keystore-csf-key.....   | 14-175 |
| 14-12 | enc-csf-key.....  | 14-175 |
| 14-13 | sign-csf-key.....   | 14-175 |
| 14-14 | keystore-csf-key.....   | 14-196 |
| 14-15 | enc-csf-key.....  | 14-196 |
| 14-16 | sign-csf-key.....   | 14-196 |
| 16-1  | ldapsearch Command to Export LDAP Identity Store.....         | 16-7   |
| 16-2  | ldapaddmt Utility to Import the Ldif File.....                | 16-7   |
| 16-3  | migrateSecurityStore - Credential Store.....                  | 16-10  |
| 16-4  | migrateSecurityStore - Policy Store.....                      | 16-12  |
| 16-5  | Export Database Utility.....                                  | 16-12  |
| 16-6  | Database Import Utility.....                                  | 16-13  |
| 16-7  | Data Pump Export Utility.....                                 | 16-14  |
| 16-8  | Database Import Utility.....                                  | 16-14  |
| 16-9  | Data Pump Utility (Export).....                               | 16-15  |
| 16-10 | Data Pump Utility (Import).....                               | 16-16  |
| 16-11 | Data Pump Utility (Export).....                               | 16-39  |
| 16-12 | Data Pump Utility (Import).....                               | 16-40  |

## List of Figures

|      |  |       |
|------|--|-------|
| 1-1  | Oracle WebCenter Architecture.....   | 1-2   |
| 1-2  | Oracle WebCenter Topology Out-of-the-Box .....                               | 1-5   |
| 1-3  | Change Center in Oracle WebLogic Server Administration Console .....         | 1-14  |
| 6-1  | Farm Home Page.....  | 6-2   |
| 6-2  | WebCenter Spaces Home Page .....   | 6-3   |
| 6-3  | WebCenter Menu for WebCenter Spaces .....                                    | 6-4   |
| 6-4  | Navigating to the WebCenter Spaces Home Page .....                           | 6-4   |
| 6-5  | Displaying the WebCenter Spaces Home Page and Menu.....                      | 6-5   |
| 6-6  | Custom WebCenter Application Home Page .....                                 | 6-5   |
| 6-7  | Navigating to a Custom WebCenter Application Home Page.....                  | 6-6   |
| 6-8  | Displaying the Custom WebCenter Application Home Page and Menu.....          | 6-7   |
| 7-1  | WLS Administration Console Home Page.....                                    | 7-3   |
| 7-2  | Summary of Servers Pane .....  | 7-4   |
| 7-3  | Create a New Server pane .....   | 7-4   |
| 7-4  | Fusion Middleware Components Page .....                                      | 7-8   |
| 7-5  | Create WebLogic Server Page .....  | 7-9   |
| 7-6  | RCU Welcome Page.....  | 7-12  |
| 7-7  | Database Connection Details Page .....                                       | 7-13  |
| 7-8  | Select Components Page .....   | 7-14  |
| 7-9  | Schema Passwords Page .....  | 7-15  |
| 7-10 | Metadata Repositories Page .....   | 7-16  |
| 7-11 | Register Database-based Metadata Repository Page.....                        | 7-16  |
| 7-12 | Select Archive Page.....   | 7-20  |
| 7-13 | Select Target Page .....   | 7-20  |
| 7-14 | Application Attributes Page .....  | 7-21  |
| 7-15 | Select Metadata Repository Window .....                                      | 7-21  |
| 7-16 | Deployment Settings Page.....  | 7-22  |
| 7-17 | Configure ADF Connections Page .....   | 7-22  |
| 7-18 | Discussion Forum Connection Settings.....                                    | 7-23  |
| 7-19 | Deployment Summary Pane .....  | 7-27  |
| 7-20 | Install Application Assistant Page.....                                      | 7-27  |
| 7-21 | Install Application Assistant - Page 2 .....                                 | 7-28  |
| 7-22 | Install Application Assistant - Page 3 .....                                 | 7-28  |
| 7-23 | Credentials Pane .....   | 7-31  |
| 7-24 | Select Application Page.....   | 7-34  |
| 7-25 | Select Archive Page.....   | 7-34  |
| 7-26 | Application Attributes Page .....  | 7-35  |
| 7-27 | Deployment Settings Page.....  | 7-36  |
| 7-28 | Configure ADF Connections Page .....   | 7-36  |
| 7-29 | Discussion Forum Connection Settings.....                                    | 7-37  |
| 7-30 | Deployment Settings Page - Deployment Plan Section.....                      | 7-37  |
| 8-1  | Managed Server Home Page.....  | 8-3   |
| 9-1  | Choosing the SOA Instance Where WebCenter Spaces Workflows are Deployed..... | 9-2   |
| 10-1 | Creating a New Provider .....  | 10-4  |
| 10-2 | Specifying Details of a New LDAP Provider.....                               | 10-5  |
| 10-3 | Configuring Content Repository Connections .....                             | 10-11 |
| 10-4 | Fusion Middleware Control WebCenter Menu.....                                | 10-21 |
| 10-5 | Manage Content Repository Connections Page .....                             | 10-21 |
| 10-6 | Edit Content Repository Connection Page.....                                 | 10-22 |
| 10-7 | Oracle WebLogic Administration Console .....                                 | 10-22 |
| 10-8 | Summary of JDBC Data Sources Page.....                                       | 10-23 |
| 10-9 | Data Source Settings Section .....   | 10-23 |
| 11-1 | Configuring Discussion and Announcement Connections .....                    | 11-5  |
| 11-2 | Creating a Virtual Directory .....   | 11-15 |

|       |   |       |
|-------|---|-------|
| 11-3  | Virtual Directory Properties .....  | 11-16 |
| 11-4  | Adding a Virtual Directory .....  | 11-16 |
| 11-5  | Virtual Directory Properties .....  | 11-17 |
| 11-6  | Configuring Instant Messaging and Presence Services.....                  | 11-18 |
| 11-7  | Configuring Mail Servers.....   | 11-28 |
| 11-8  | Configuring Oracle Secure Search Services .....                           | 11-38 |
| 11-9  | Configuring Worklist Connections .....                                    | 11-46 |
| 11-10 | Oracle WebCenter Wiki and Blog Server Interface.....                      | 11-55 |
| 11-11 | Administration Link .....   | 11-55 |
| 11-12 | Administration Mode.....  | 11-56 |
| 11-13 | Adding a New Domain.....  | 11-59 |
| 11-14 | List of Domains .....   | 11-59 |
| 11-15 | Domain Menu.....  | 11-60 |
| 11-16 | Menu of a New Domain.....   | 11-61 |
| 11-17 | Editing a Domain Menu.....  | 11-62 |
| 11-18 | Adding a Domain Member.....   | 11-63 |
| 11-19 | Restricting Access to Domain Members .....                                | 11-63 |
| 11-20 | Selecting a Theme .....   | 11-64 |
| 11-21 | Managing Templates .....  | 11-64 |
| 11-22 | Creating a Page Based on a Template.....                                  | 11-65 |
| 11-23 | Unlocking a Page .....  | 11-66 |
| 11-24 | Adding a User .....   | 11-66 |
| 11-25 | Editing a Role .....  | 11-67 |
| 11-26 | Specifying Permissions for a Role .....                                   | 11-68 |
| 11-27 | Enabling Anonymous Access .....   | 11-68 |
| 11-28 | Blocking an IP Address.....   | 11-69 |
| 11-29 | Deleting a Wiki Page .....  | 11-70 |
| 11-30 | Configuration Page.....   | 11-71 |
| 11-31 | Wiki and Blog Server Settings.....  | 11-72 |
| 13-1  | Edit External Application .....   | 13-2  |
| 13-2  | Configuring External Application Connections.....                         | 13-4  |
| 14-1  | Basic WebCenter Application Architecture .....                            | 14-2  |
| 14-2  | WebCenter Application Architecture with Back-end Server Connections ..... | 14-2  |
| 14-3  | WebCenter Spaces Security Layers .....                                    | 14-2  |
| 14-4  | Domain Structure Pane .....   | 14-11 |
| 14-5  | Summary of Security Realms pane .....                                     | 14-12 |
| 14-6  | Realm Settings Pane .....   | 14-12 |
| 14-7  | Settings Pane - Providers .....   | 14-13 |
| 14-8  | Create a New Authentication Provider Pane.....                            | 14-13 |
| 14-9  | Settings Pane - Authentication Providers.....                             | 14-14 |
| 14-10 | Settings Pane for Authenticator .....                                     | 14-15 |
| 14-11 | Provider Specific Pane.....   | 14-16 |
| 14-12 | Domain Structure Pane .....   | 14-19 |
| 14-13 | Summary of Security Realms pane .....                                     | 14-19 |
| 14-14 | Realm Settings Pane .....   | 14-20 |
| 14-15 | Create a New User Page .....  | 14-21 |
| 14-16 | Domain Structure Pane (wc_domain).....                                    | 14-22 |
| 14-17 | Settings Pane with Embedded LDAP Settings .....                           | 14-23 |
| 14-18 | Embedded LDAP Directory Information Tree .....                            | 14-23 |
| 14-19 | Domain Structure Pane .....   | 14-27 |
| 14-20 | Summary of Security Realms pane .....                                     | 14-27 |
| 14-21 | Realm Settings Pane .....   | 14-28 |
| 14-22 | Realm Roles Settings Pane.....  | 14-29 |
| 14-23 | Edit Global Role Page.....  | 14-30 |
| 14-24 | Edit Global Role Page - Predicate List .....                              | 14-30 |

|       |  |        |
|-------|--|--------|
| 14-25 | Edit Global Role Page - Arguments .....                      | 14-31  |
| 14-26 | Application Roles Page .....                                 | 14-32  |
| 14-27 | Edit Application Role Page.....                              | 14-33  |
| 14-28 | Add User Pop-up .....  | 14-33  |
| 14-29 | Security Provider Configuration Page.....                    | 14-39  |
| 14-30 | Set Security Provider Page.....                              | 14-40  |
| 14-31 | Keystores Settings Pane .....                                | 14-44  |
| 14-32 | Summary of Servers Pane .....                                | 14-45  |
| 14-33 | Settings Pane for WebCenter Spaces Server .....              | 14-46  |
| 14-34 | Keystores Pane .....   | 14-47  |
| 14-35 | General Configuration Pane.....                              | 14-48  |
| 14-36 | Advanced SSL Configuration Settings .....                    | 14-49  |
| 14-37 | Control Settings Pane .....                                  | 14-50  |
| 14-38 | General Configuration Pane.....                              | 14-51  |
| 14-39 | Advanced SSL Configuration Settings .....                    | 14-52  |
| 14-40 | Summary of Servers Pane.....                                 | 14-55  |
| 14-41 | Settings Pane for Services Server .....                      | 14-56  |
| 14-42 | Keystores Pane .....   | 14-57  |
| 14-43 | Control Settings Pane .....                                  | 14-58  |
| 14-44 | General Configuration Pane.....                              | 14-59  |
| 14-45 | Advanced SSL Configuration Settings .....                    | 14-60  |
| 14-46 | Summary of Servers Pane.....                                 | 14-61  |
| 14-47 | Settings Pane for Portlet Server .....                       | 14-62  |
| 14-48 | Keystores Pane .....   | 14-63  |
| 14-49 | Control Settings Pane .....                                  | 14-64  |
| 14-50 | Summary of Servers Pane.....                                 | 14-66  |
| 14-51 | Settings Pane (WLS_Spaces Server) .....                      | 14-67  |
| 14-52 | OAM Single Sign-On Components and Topology .....             | 14-73  |
| 14-53 | Policy Manager Pane .....                                    | 14-79  |
| 14-54 | Create Policy Domain Page .....                              | 14-80  |
| 14-55 | Policy Domain Resource Page.....                             | 14-80  |
| 14-56 | Authorization Rules Page .....                               | 14-81  |
| 14-57 | Allow Access Page .....                                      | 14-82  |
| 14-58 | Access Manager Authentication Rules Page.....                | 14-82  |
| 14-59 | Authorization Expression Page .....                          | 14-83  |
| 14-60 | Actions Page .....   | 14-84  |
| 14-61 | Policies Page .....  | 14-85  |
| 14-62 | Summary of Security Realms Pane .....                        | 14-86  |
| 14-63 | Settings Pane.....   | 14-86  |
| 14-64 | Settings Pane - Providers .....                              | 14-87  |
| 14-65 | Create a New Authentication Provider Pane.....               | 14-87  |
| 14-66 | Common Settings Pane .....                                   | 14-88  |
| 14-67 | Provider Specific Settings for OID Authenticator .....       | 14-89  |
| 14-68 | Summary of Security Realms Pane .....                        | 14-90  |
| 14-69 | Settings Pane.....   | 14-91  |
| 14-70 | Settings Pane - Providers .....                              | 14-91  |
| 14-71 | Create a New Authentication Provider Pane.....               | 14-92  |
| 14-72 | Common Settings Pane .....                                   | 14-92  |
| 14-73 | Provider Specific Settings for the OAMIdentityAsserter ..... | 14-93  |
| 14-74 | Policy Manager Pane .....                                    | 14-95  |
| 14-75 | Policy Domain Resource Page.....                             | 14-96  |
| 14-76 | Deployment Summary Pane .....                                | 14-97  |
| 14-77 | Security Filter Settings Page .....                          | 14-99  |
| 14-78 | OSSO Components and Topology .....                           | 14-101 |
| 14-79 | Summary of Security Realms Pane .....                        | 14-102 |

|        |  |        |
|--------|--|--------|
| 14-80  | Settings Pane.....   | 14-103 |
| 14-81  | Settings Pane - Providers .....  | 14-103 |
| 14-82  | Create a New Authentication Provider Pane.....                                       | 14-104 |
| 14-83  | Detailed SAML Single Sign-on Components and Topology (POST Profile Configured) ..... | 14-108 |
| 14-84  | SAML Single Sign-on Components and Topology (POST Profile Configured) .....          | 14-109 |
| 14-85  | Summary of Servers Pane .....  | 14-112 |
| 14-86  | Settings Pane for WebCenter Spaces Server .....                                      | 14-113 |
| 14-87  | Keystores Pane .....   | 14-114 |
| 14-88  | Summary of Security Realms Pane .....  | 14-115 |
| 14-89  | Security Realm Settings Page .....   | 14-116 |
| 14-90  | Credential Mapping Pane.....   | 14-116 |
| 14-91  | Create a New Credential Provider Pane .....  | 14-117 |
| 14-92  | Provider Settings Pane .....   | 14-117 |
| 14-93  | Provider Specific Settings Pane.....   | 14-118 |
| 14-94  | Summary of Security Realms Pane .....  | 14-119 |
| 14-95  | Credential Mapping Providers Settings Pane.....                                      | 14-120 |
| 14-96  | Relying Parties Management Settings Pane.....  | 14-120 |
| 14-97  | Create a New Relying Party Page.....   | 14-121 |
| 14-98  | Relying Party Settings Page.....   | 14-122 |
| 14-99  | Summary of Servers Page .....  | 14-128 |
| 14-100 | Federation Services Configuration SAML 1.1 Source Site Settings Page .....           | 14-129 |
| 14-101 | Summary of Security Realms Pane .....  | 14-131 |
| 14-102 | Security Realm Settings Page .....   | 14-131 |
| 14-103 | Authentication Settings Pane .....   | 14-132 |
| 14-104 | Create a New Authentication Provider Page.....                                       | 14-132 |
| 14-105 | Summary of Security Realms Pane .....  | 14-133 |
| 14-106 | Security Realm Settings Page .....   | 14-134 |
| 14-107 | Authentication Settings Pane .....   | 14-135 |
| 14-108 | Certificate Settings Pane .....  | 14-135 |
| 14-109 | Create a New Identity Asserter Certificate Page.....                                 | 14-136 |
| 14-110 | Summary of Security Realms Pane .....  | 14-137 |
| 14-111 | Security Realm Settings Page .....   | 14-137 |
| 14-112 | Authentication Settings Pane .....   | 14-138 |
| 14-113 | Asserting Parties Settings Pane.....   | 14-138 |
| 14-114 | Create a New Asserting Party Page .....  | 14-139 |
| 14-115 | Asserting Party Settings Page .....  | 14-140 |
| 14-116 | Summary of Servers Page .....  | 14-149 |
| 14-117 | SAML 1.1 Destination Site Settings Pane (Wiki and Discussions) .....                 | 14-150 |
| 14-118 | SAML 1.1 Destination Site Settings Pane (RSS).....                                   | 14-152 |
| 14-119 | SAML 1.1 Destination Site Settings Pane (Worklist Detail and SDP) .....              | 14-153 |
| 14-120 | Connecting to a Server Through a Key Distribution Center .....                       | 14-156 |
| 14-121 | SPNEGO-based Authentication.....   | 14-157 |
| 14-122 | Configuring SSO with Microsoft Clients.....  | 14-158 |
| 14-123 | Summary of Security Realms Pane .....  | 14-159 |
| 14-124 | Security Realm Settings Page .....   | 14-160 |
| 14-125 | Authentication Settings Pane .....   | 14-161 |
| 14-126 | Create a New Authentication Provider Pane.....                                       | 14-161 |
| 14-127 | Summary of Security Realms Pane .....  | 14-162 |
| 14-128 | Security Realm Settings Page .....   | 14-163 |
| 14-129 | Authentication Settings Pane .....   | 14-164 |
| 14-130 | Create a New Authentication Provider Pane.....                                       | 14-164 |
| 14-131 | Provider Settings Page .....   | 14-165 |
| 14-132 | Provider Specific Settings Pane.....   | 14-166 |
| 14-133 | Web Services Summary Page.....   | 14-182 |

|        |   |        |
|--------|---|--------|
| 14-134 | Web Service Endpoints Page .....                    | 14-183 |
| 14-135 | Web Services Endpoint Policies Page .....           | 14-183 |
| 14-136 | Attach/Detach Policies Page .....                   | 14-184 |
| 14-137 | Attach Detach Policy Page with Policy Attached..... | 14-185 |
| 14-138 | Security Provider Configuration Page.....           | 14-189 |
| 14-139 | Keystore Configuration Page .....                   | 14-189 |
| 14-140 | Security Provider Configuration Page.....           | 14-190 |
| 14-141 | Keystore Configuration Page .....                   | 14-191 |
| 14-142 | Security Provider Configuration Page.....           | 14-195 |
| 14-143 | Keystore Configuration Page .....                   | 14-195 |
| 14-144 | Credentials Page.....                               | 14-197 |
| 14-145 | Credentials Pane .....                              | 14-198 |
| 14-146 | Credentials Pane with New Shared Key .....          | 14-199 |
| 14-147 | System Policies Pane.....                           | 14-201 |
| 14-148 | Create System Grant Pane .....                      | 14-201 |
| 14-149 | Add Permission Pane .....                           | 14-202 |
| 15-1   | Announcement Metrics.....                           | 15-9   |
| 15-2   | BPEL Worklist Metrics .....                         | 15-10  |
| 15-3   | Content Repository Metrics.....                     | 15-11  |
| 15-4   | Content Repository Metrics - Per Operation .....    | 15-11  |
| 15-5   | Discussion Metrics .....                            | 15-15  |
| 15-6   | Group Space Events Metrics .....                    | 15-18  |
| 15-7   | External Application Metrics .....                  | 15-19  |
| 15-8   | External Application Metrics - Per Operation .....  | 15-20  |
| 15-9   | IMP Metrics.....                                    | 15-21  |
| 15-10  | Import/Export Metrics .....                         | 15-22  |
| 15-11  | List Metrics.....                                   | 15-23  |
| 15-12  | Mail Metrics .....                                  | 15-25  |
| 15-13  | Notes Metrics.....                                  | 15-26  |
| 15-14  | Page Metrics.....                                   | 15-27  |
| 15-15  | Portlet Producer Metrics .....                      | 15-28  |
| 15-16  | Portlet Metrics .....                               | 15-31  |
| 15-17  | RSS News Feed Metrics.....                          | 15-34  |
| 15-18  | Recent Activity Metrics.....                        | 15-35  |
| 15-19  | Search Metrics.....                                 | 15-35  |
| 15-20  | Group Space Metrics .....                           | 15-40  |
| 16-1   | Information Exported with WebCenter Spaces.....     | 16-2   |
| 16-2   | WebCenter Menu - Application Export Option .....    | 16-18  |
| 16-3   | Select the Archive to be Exported.....              | 16-18  |
| 16-4   | Download.....                                       | 16-20  |
| 16-5   | WebCenter Spaces Application Import Page.....       | 16-21  |
| 16-6   | WebCenter Spaces Application Import dialog .....    | 16-21  |
| 16-7   | Exporting Group Space Discussions .....             | 16-24  |
| 16-8   | Importing Group Space Discussions.....              | 16-26  |
| 16-9   | Editing Forum Permissions .....                     | 16-27  |
| 16-10  | WebCenter Application Export and Import .....       | 16-34  |
| 17-1   | Administration Link .....                           | 17-1   |
| 17-2   | WebCenter Administration Pages .....                | 17-2   |
| 18-1   | Naming Your WebCenter .....                         | 18-2   |
| 18-2   | Customizing the Help Link .....                     | 18-2   |
| 18-3   | The Sidebar .....                                   | 18-3   |
| 18-4   | Customizing the Sidebar.....                        | 18-4   |
| 18-5   | Controlling Sidebar Personalization .....           | 18-5   |
| 18-6   | Changing the WebCenter Logo .....                   | 18-6   |
| 18-7   | Customizing the Copyright and Privacy URL .....     | 18-8   |

|       |  |       |
|-------|--|-------|
| 18-8  | Setting Discussion Forum Options.....                          | 18-10 |
| 18-9  | Personal Profile .....   | 18-14 |
| 18-10 | Profile Management Settings .....                              | 18-15 |
| 18-11 | Application Templates - chromeLevel Options.....               | 18-18 |
| 18-12 | Standard Page Styles .....                                     | 18-19 |
| 19-1  | Application Roles - Default Discussion Permissions.....        | 19-6  |
| 19-2  | Group Space Roles - Default Discussion Permissions.....        | 19-6  |
| 19-3  | WebCenter Administration - Users Page .....                    | 19-7  |
| 19-4  | Find User Icon .....   | 19-7  |
| 19-5  | Finding Users and Groups in the identity store.....            | 19-8  |
| 19-6  | Assigning a User Role .....                                    | 19-8  |
| 19-7  | Changing a User's Application Role .....                       | 19-9  |
| 19-8  | Changing a User's Application Role .....                       | 19-10 |
| 19-9  | WebCenter Administration - Roles Page.....                     | 19-12 |
| 19-10 | Creating a New Role.....                                       | 19-13 |
| 19-11 | Deleting an Application Role .....                             | 19-15 |
| 19-12 | Allowing Self-Registration Through Invitations.....            | 19-17 |
| 19-13 | Self-Registration Available on Login Form.....                 | 19-18 |
| 19-14 | Allowing Self-Registration Through Invitations.....            | 19-18 |
| 20-1  | Welcome Page - Out-of-the-box Business Role Page.....          | 20-2  |
| 20-2  | Viewing Business Role Pages.....                               | 20-3  |
| 20-3  | Setting Access Permissions for a Business Role Pages .....     | 20-4  |
| 20-4  | Setting Page Access.....                                       | 20-5  |
| 20-5  | Choosing Who Can See the Business Role Page.....               | 20-5  |
| 20-6  | Editing Default Page Permissions .....                         | 20-6  |
| 20-7  | Choosing a Default Display Order for Business Role Pages ..... | 20-7  |
| 20-8  | Editing Business Role Pages.....                               | 20-8  |
| 20-9  | Copying a Business Role Page .....                             | 20-9  |
| 20-10 | Naming the New Page .....                                      | 20-9  |
| 20-11 | Deleting Business Role Pages.....                              | 20-10 |
| 20-12 | Setting Page Defaults For Everyone .....                       | 20-11 |
| 20-13 | Setting Page Defaults.....                                     | 20-11 |
| 20-14 | Editing Personal Pages.....                                    | 20-13 |
| 20-15 | Editing Page Access.....                                       | 20-14 |
| 20-16 | Setting Page Access.....                                       | 20-14 |
| 20-17 | Copying a Personal Page .....                                  | 20-15 |
| 20-18 | Naming the New Page .....                                      | 20-16 |
| 20-19 | Deleting Personal Pages.....                                   | 20-17 |
| 20-20 | Public Welcome Page .....                                      | 20-18 |
| 20-21 | Default Login Page .....                                       | 20-19 |
| 20-22 | Edit Icon for Login Page .....                                 | 20-19 |
| 20-23 | Customizing the Login Page .....                               | 20-20 |
| 20-24 | Default Self-Registration Page .....                           | 20-20 |
| 20-25 | Edit Icon for Self-Registration Page .....                     | 20-21 |
| 20-26 | Customizing the Self-Registration Page .....                   | 20-21 |
| 21-1  | Sidebar - Applications Pane .....                              | 21-2  |
| 21-2  | Applications Pane - Edit Icon.....                             | 21-3  |
| 21-3  | Editing the Applications Pane .....                            | 21-3  |
| 21-4  | Choosing an Application .....                                  | 21-4  |
| 21-5  | Editing Application Links .....                                | 21-4  |
| 21-6  | Editing Application Links .....                                | 21-6  |
| 21-7  | Arranging the Applications List.....                           | 21-6  |
| 21-8  | Editing Application Links.....                                 | 21-7  |
| 22-1  | WebCenter Administration - Group Spaces .....                  | 22-2  |
| 22-2  | About Group Space .....  | 22-2  |

|      |  |      |
|------|--|------|
| 22-3 | Taking a Group Space Offline .....               | 22-3 |
| 22-4 | Bringing a Group Space Online .....              | 22-4 |
| 22-5 | Closing a Group Space .....                      | 22-5 |
| 22-6 | Activating a Group Space .....                   | 22-5 |
| 22-7 | Deleting a Group Space.....                      | 22-6 |
| 22-8 | WebCenter Administration - Templates Page .....  | 22-7 |
| 22-9 | Deleting a Group Space Template .....            | 22-8 |
| 23-1 | Exporting Group Spaces .....                     | 23-2 |
| 23-2 | Exporting Group Spaces In Progress .....         | 23-4 |
| 23-3 | Importing Group Spaces .....                     | 23-5 |
| 23-4 | Exporting Group Space Templates.....             | 23-6 |
| 23-5 | Exporting Group Space Templates In Progress..... | 23-7 |
| 23-6 | Importing Group Space Templates .....            | 23-8 |
| B-1  | Application Defined MBeans .....                 | B-3  |



## List of Tables

|       |  |       |
|-------|--|-------|
| 1-1   | Oracle WebCenter Managed Servers and Applications.....   | 1-6   |
| 1-2   | External Resources - Access Types.....   | 1-7   |
| 1-3   | Oracle WebCenter Configuration Files.....  | 1-7   |
| 1-4   | Oracle WebCenter Configuration Location .....  | 1-8   |
| 1-5   | WebCenter Operations and Oracle WebLogic Server Roles .....                                      | 1-10  |
| 1-6   | WebCenter Operations and Administration Tools.....   | 1-11  |
| 2-1   | Roadmap - Setting Up WebCenter Spaces for the First Time .....                                   | 2-3   |
| 2-2   | Roadmap - Customizing WebCenter Spaces for the First Time .....                                  | 2-5   |
| 3-1   | Roadmap - Administering and Monitoring WebCenter Spaces .....                                    | 3-2   |
| 3-2   | Roadmap - Keeping WebCenter Spaces Up and Running .....  | 3-5   |
| 4-1   | Roadmap - Getting Custom WebCenter Applications Up and Running for the First Time...<br>4-2      |       |
| 5-1   | Roadmap - Maintaining Custom WebCenter Applications .....  | 5-1   |
| 7-1   | Information Artifact Target Stores .....   | 7-18  |
| 10-1  | Oracle WebCenter-Specific Postinstallation Configuration Tasks for Oracle Content Server<br>10-3 |       |
| 10-2  | Manage Content Repository Connections.....   | 10-11 |
| 10-3  | Content Repository Connection - WebCenter Spaces Repository Details.....                         | 10-12 |
| 10-4  | Oracle Content Server Connection Parameters .....  | 10-13 |
| 10-5  | Oracle Portal Connection Parameters .....  | 10-14 |
| 10-6  | File System Connection Parameters.....   | 10-15 |
| 10-7  | Content Repository Connection - WebCenter Spaces Repository Details.....                         | 10-20 |
| 11-1  | Discussion and Announcement Connection - Name.....   | 11-5  |
| 11-2  | Discussion and Announcement Connection - Connection Details.....                                 | 11-5  |
| 11-3  | Discussion and Announcement Connection - Advanced Configuration .....                            | 11-6  |
| 11-4  | Additional Discussion Connection Properties .....  | 11-6  |
| 11-5  | Discussion and Announcement Connection - Additional Properties .....                             | 11-7  |
| 11-6  | Instant Messaging and Presence Connection - Name .....   | 11-19 |
| 11-7  | Instant Messaging and Presence Connection - Connection Details .....                             | 11-19 |
| 11-8  | Additional IMP Connection Properties .....   | 11-21 |
| 11-9  | Instant Messaging and Presence Connection - Additional Properties.....                           | 11-22 |
| 11-10 | Mail Server Connection - Name.....   | 11-29 |
| 11-11 | Mail Server Connection Parameters.....   | 11-29 |
| 11-12 | LDAP Directory Server Configuration Parameters .....   | 11-30 |
| 11-13 | Mail Server Connection - Advanced Configuration .....  | 11-31 |
| 11-14 | Additional Mail Connection Properties.....   | 11-31 |
| 11-15 | Mail Connection - Additional Properties .....  | 11-32 |
| 11-16 | Search Connection - Name .....   | 11-38 |
| 11-17 | Oracle Secure Enterprise Search - Connection Details .....                                       | 11-38 |
| 11-18 | Oracle Secure Enterprise Search - Advanced Configuration.....                                    | 11-39 |
| 11-19 | Worklist Connection - Name.....  | 11-46 |
| 11-20 | Worklist Connection - Connection Details.....  | 11-47 |
| 11-21 | WebCenter Web 2.0 Services Storing Content in WebCenter Repository .....                         | 11-52 |
| 11-22 | Links in the General Menu .....  | 11-55 |
| 11-23 | Links in the Administration Mode of Oracle WebCenter Wiki and Blog Server .....                  | 11-56 |
| 12-1  | WSRP Producer Connection Parameters.....   | 12-3  |
| 12-2  | WSRP Producer Security Connection Parameters .....   | 12-5  |
| 12-3  | WSRP Producer Key Store Connection Parameters.....   | 12-6  |
| 12-4  | Oracle PDK-Java Producer Connection Parameters .....   | 12-8  |
| 13-1  | External Application Connection - Name .....   | 13-4  |
| 13-2  | External Application Connection - Login Details .....  | 13-4  |
| 13-3  | External Application Connection - Authentication Details .....                                   | 13-6  |
| 13-4  | External Application Connection - Additional Login Fields.....                                   | 13-6  |

|       |  |        |
|-------|--|--------|
| 13-5  | External Application Connection - Shared User and Public User Credentials..... | 13-7   |
| 14-1  | WebCenter Role Permissions .....   | 14-6   |
| 14-2  | Sample Settings for AccessGate Entry .....                                     | 14-77  |
| 14-3  | SAML Credential Mapping Provider Security Realm Settings.....                  | 14-118 |
| 14-4  | Relying Party Settings for Wiki Service.....                                   | 14-122 |
| 14-5  | Relying Party Settings for Worklist Community Detail.....                      | 14-123 |
| 14-6  | Relying Party Settings for Worklist SDP .....                                  | 14-124 |
| 14-7  | Relying Party Settings for Worklist Integration .....                          | 14-125 |
| 14-8  | Relying Party Settings for RSS .....   | 14-126 |
| 14-9  | Relying Party Settings for Discussions .....                                   | 14-127 |
| 14-10 | Source Site Federation Services Parameters.....                                | 14-129 |
| 14-11 | Certificates Page Parameters.....  | 14-136 |
| 14-12 | WC Domain - Asserting Party for Wiki.....                                      | 14-140 |
| 14-13 | WC Domain - Asserting Party for RSS .....                                      | 14-142 |
| 14-14 | WC Domain - Asserting Party for RSS .....                                      | 14-143 |
| 14-15 | SOA Domain - Asserting Party for Worklist Community Detail .....               | 14-144 |
| 14-16 | SOA Domain - Asserting Party for Worklist SDP.....                             | 14-146 |
| 14-17 | In SOA Domain, Asserting party For Worklist Integration.....                   | 14-147 |
| 14-18 | SAML Destination Site Attributes (Wiki and Discussions) .....                  | 14-150 |
| 14-19 | SAML Destination Site Attributes (RSS).....                                    | 14-152 |
| 14-20 | SOA Domain - SAML Destination Site Attributes (Worklist Detail and SDP) .....  | 14-154 |
| 14-21 | Active Directory Authenticator Settings .....                                  | 14-166 |
| 15-1  | Common Performance Metrics .....   | 15-3   |
| 15-2  | Description of Common Metrics - Summary (All Operations).....                  | 15-6   |
| 15-3  | Description of Common Metrics - Per Operation .....                            | 15-7   |
| 15-4  | Announcements Service - Operations Monitored.....                              | 15-9   |
| 15-5  | Documents Service - Operations Monitored.....                                  | 15-11  |
| 15-6  | Content Repository Metrics - Summary (All Repositories).....                   | 15-12  |
| 15-7  | Content Repository Metrics - Operation Summary Per Repository.....             | 15-14  |
| 15-8  | Content Repository Metrics - Operation Detail Per Repository .....             | 15-15  |
| 15-9  | Discussions Service - Operations Monitored .....                               | 15-16  |
| 15-10 | Events Service - Operations Monitored.....                                     | 15-18  |
| 15-11 | External Applications - Operations Monitored .....                             | 15-20  |
| 15-12 | Instant Messaging and Presence Service - Operations Monitored .....            | 15-21  |
| 15-13 | Import/Export - Operations Monitored.....                                      | 15-22  |
| 15-14 | List service - Operations Monitored.....                                       | 15-23  |
| 15-15 | Mail Service - Operations Monitored.....                                       | 15-25  |
| 15-16 | Notes Service - Operations Monitored .....                                     | 15-26  |
| 15-17 | Page Service - Operations Monitored .....                                      | 15-27  |
| 15-18 | Portlet Producers - Summary .....  | 15-28  |
| 15-19 | Portlet Producer -Detail .....   | 15-29  |
| 15-20 | Portlets - Summary .....   | 15-31  |
| 15-21 | Portlet - Detail.....  | 15-32  |
| 15-22 | Portlet - HTTP Response Code Statistics.....                                   | 15-33  |
| 15-23 | HTTP Response Codes.....   | 15-33  |
| 15-24 | Search Service - Search Sources .....  | 15-35  |
| 15-25 | Group Space Metrics .....  | 15-41  |
| 16-1  | WebCenter Spaces - Service Customizations.....                                 | 16-3   |
| 16-2  | WebCenter Spaces Application General Settings.....                             | 16-6   |
| 16-3  | WebCenter Spaces Application Export Options .....                              | 16-19  |
| 16-4  | Custom WebCenter Application Migration Tools.....                              | 16-34  |
| 18-1  | Languages Available for Oracle WebCenter Spaces.....                           | 18-9   |
| 18-2  | WebCenter Services .....   | 18-16  |
| 19-1  | Default Administrator in WebCenter Spaces .....                                | 19-2   |
| 19-2  | Default Application Roles for WebCenter Spaces.....                            | 19-3   |

|      |  |      |
|------|--|------|
| 19-3 | Application Permissions in WebCenter Spaces.....                 | 19-4 |
| 19-4 | Discussions Server Roles and Permissions - Application.....      | 19-5 |
| 19-5 | Discussions Server Roles and Permissions - For Group Spaces..... | 19-5 |
| 21-1 | Application Link Properties .....                                | 21-5 |
| 23-1 | Group Space Export Options .....                                 | 23-3 |
| B-1  | File Names and WLST Commands for Web 2.0 Services.....           | B-5  |



---

---

# Preface

Welcome to the Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter! This guide describes how to administer Oracle WebCenter, WebCenter Spaces, and custom WebCenter application deployments. It describes how to start and stop WebCenter applications, how to configure WebCenter components, back-end services, and security, as well as how to back up, recover, and migrate WebCenter applications and WebCenter Web 2.0 Services.

This guide also contains a section for WebCenter Spaces administrators that describes how to customize WebCenter Spaces out-of-the-box, and how to manage user roles and responsibilities for this application.

## Audience

This document is intended for:

- Fusion Middleware administrators responsible for Oracle WebCenter installations, and WebCenter application deployments (including WebCenter Spaces).
- WebCenter Spaces administrators (users granted the Administrator role through WebCenter Spaces Administration).

This guide assumes that the audience is familiar with the concepts and content described in *Oracle Fusion Middleware Administrator's Guide*.

## Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at <http://www.oracle.com/accessibility/>.

### Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

### Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

### Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at

<http://www.fcc.gov/cgb/consumerfacts/trs.html>, and a list of phone numbers is available at <http://www.fcc.gov/cgb/dro/trsphonebk.html>.

## Related Documents

For more information, see the following documents in the Oracle Fusion Middleware 11g Release 1 (11.1.1) documentation set:

- *Oracle Fusion Middleware Administrator's Guide*
- *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*
- *Oracle Fusion Middleware User's Guide for Oracle WebCenter*
- *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*
- *Oracle Fusion Middleware Tutorial for Oracle WebCenter Developers*

## Conventions

The following text conventions are used in this document:

| Convention      | Meaning  |
|-----------------|--|
| <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. |

# Part I

---

## Understanding Oracle WebCenter

This part of the Administrator's Guide introduces you to Oracle WebCenter and its administration tools.

Part I contains the following chapters:

- [Chapter 1, "Introduction to Oracle WebCenter Administration"](#)





---

---

# Introduction to Oracle WebCenter Administration

Welcome to Oracle WebCenter!

This chapter provides a high-level overview of Oracle WebCenter and its administrative tools. It includes the following sections:

- [Introducing Oracle WebCenter](#)
- [Oracle WebCenter Architecture](#)
- [Oracle WebCenter Topology](#)
- [Oracle WebCenter Spaces](#)
- [Custom WebCenter Applications](#)
- [Planning WebCenter Installations](#)
- [Understanding the WebCenter 11g Installation](#)
- [Understanding Administrative Operations, Roles, and Tools](#)
- [Performance Monitoring and Diagnostics](#)
- [WebCenter Application Deployment](#)
- [Data Migration, Backup, and Recovery](#)
- [Oracle WebCenter Administration Tools](#)

## 1.1 Introducing Oracle WebCenter

Oracle WebCenter is an integrated set of components with which you can create social applications, enterprise portals, collaborative communities, and composite applications, built on a standards-based, service-oriented architecture. Oracle WebCenter combines dynamic user interface technologies with which to develop rich internet applications, the flexibility and power of an integrated, multi-channel portal framework, and a set of horizontal Enterprise 2.0 capabilities delivered as services that provide content, collaboration, presence and social networking capabilities. Based on these components, Oracle WebCenter also provides an out-of-the-box enterprise-ready customizable application, WebCenter Spaces, with a configurable work environment that enables individuals and groups to work and collaborate more effectively.

Oracle WebCenter provides an open and extensible solution that allows users to interact directly with services like instant messaging, documents, content management, discussion forums, wikis and tagging directly from within the context of

a portal or an application. These tools and services empower end users and IT to build and deploy next-generation collaborative applications and portals.

This section describes Oracle WebCenter components and architecture in the following sections:

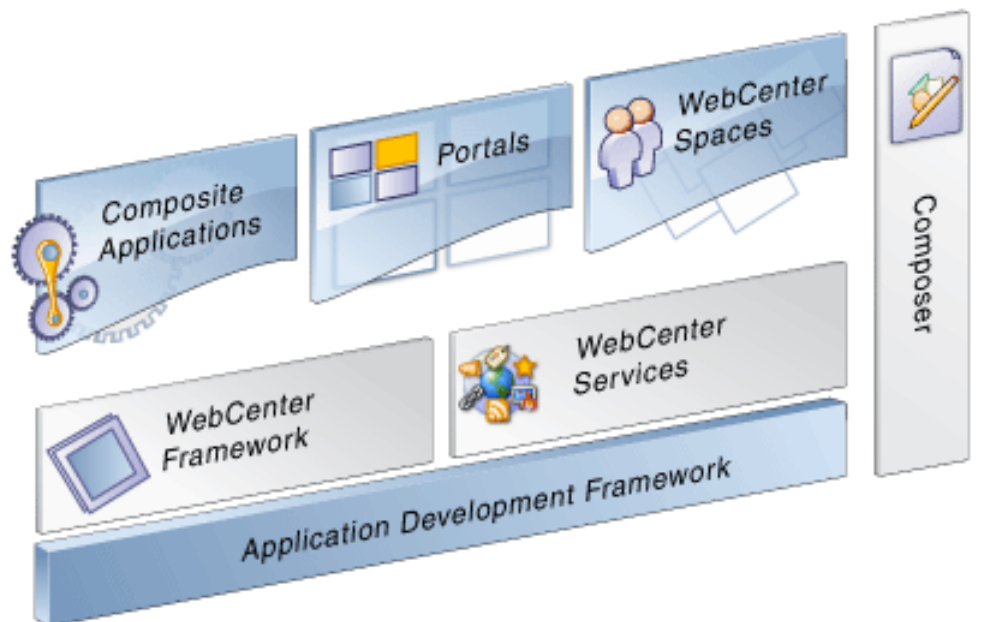
- [Section 1.2, "Oracle WebCenter Architecture"](#)
- [Section 1.3, "Oracle WebCenter Topology"](#)
- [Section 1.4, "Oracle WebCenter Spaces"](#)
- [Section 1.5, "Custom WebCenter Applications"](#)

## 1.2 Oracle WebCenter Architecture

Oracle WebCenter comprises the following components (shown in [Figure 1-1](#)):

- [WebCenter Framework](#)
- [Application Developer Framework](#)
- [WebCenter Web 2.0 Services](#)
- [WebCenter Composer](#)
- [WebCenter Spaces](#)
- [Portals](#)
- [Composite Applications](#)

*Figure 1-1 Oracle WebCenter Architecture*



### 1.2.1 WebCenter Framework

Injects portal capabilities into ADF, including:

- Run-time customization (you can make in-place changes to the application without re-deploying it)
- Support for JSR-168 standards-based WSRP portlets, and PDK-Java portlets
- Content integration through JCR (JSR170), including Oracle Content Server (OCS), file system, and Oracle Portal
- Oracle JSF Portlet Bridge, which lets you expose JSF pages and ADF task flows as standards-based portlets

## 1.2.2 Application Developer Framework

Application Developer Framework (ADF) is a productivity layer that sits on top of JSF and provides:

- Unified access to back ends such as databases, Web services, XML, CSV, and BPEL
- Data binding (JSR 227) connecting the user interface with back-end data controls
- Over 100 data-aware JSF view components
- Native component model that includes task flows
- Fine grained JAAS security model

## 1.2.3 WebCenter Web 2.0 Services

WebCenter Web 2.0 services provides:

- Seamless integration with enterprise-level Web 2.0 services
- Thin adapter layer to abstract back-end services. For example:
  - Content adapter: Oracle Content Server and Oracle Portal
  - Presence Adapter: Oracle WebLogic Communication Server (OWLCS), Microsoft Live Communication Server
- Back-end systems represented by a unified connection architecture
- User interface to services presented through rich task flow components

## 1.2.4 WebCenter Composer

WebCenter Composer provides:

- Ability to perform run-time customization in-place in your browser
- A rich, intuitive user experience where you can:
  - Browse and add resources to pages
  - Re-arrange page layout
  - Set page and component properties
  - Contextually wire components

## 1.2.5 WebCenter Spaces

Built using JSF, ADF, WebCenter Framework, WebCenter Web 2.0 services, and Composer, WebCenter Spaces provides:

- A browser-based, community-focused portal framework targeting the business user.
- A personal space for each user, providing a private work area for storing personal content, keeping notes, viewing and responding to business process assignments, maintaining a list of online buddies, emailing, and so on. The focus of a personal space is personal productivity.
- Group spaces, a rich team collaboration platform.
- Threaded discussions, blogs, wikis, worklists, announcements, RSS, recent activities, search, and more.

## 1.2.6 Portals

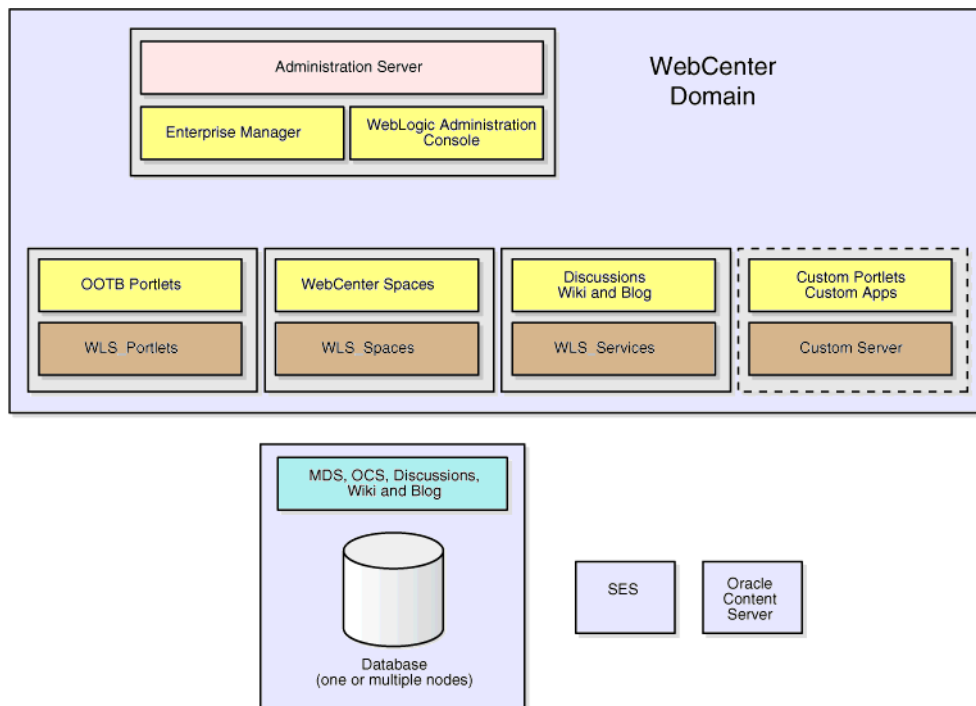
Portals provide a common interface (a Web page) to a personalized, single point of interaction with Web-based applications and information relevant to individual users or class of users. For information about creating portals, see *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

## 1.2.7 Composite Applications

A composite application is an assembly of services, service components, wires, and references designed and deployed as a single application. For more information about composite applications, see the *Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite*.

## 1.3 Oracle WebCenter Topology

Oracle WebCenter installation creates a WebCenter Oracle home under the Oracle Middleware home directory. The installation also creates a WebCenter domain (`wc_domain`), containing the administration server and three managed servers, as shown in [Figure 1-2](#). Note that applications are shown in yellow, while the managed servers they run on are shown in brown.

**Figure 1–2 Oracle WebCenter Topology Out-of-the-Box**

Out-of-the-box managed servers host the following components:

- WLS\_Spaces - WebCenter Spaces
- WLS\_Portlets - WebCenter Portlets
- WLS\_Services - Oracle WebCenter Discussions Server, the Oracle WebCenter Wiki and Blog Server, and any additional WebCenter Web 2.0 services that you choose to integrate

An optional fourth managed server (an applications server) can be used to run custom WebCenter applications. When you create additional managed servers, they are provisioned with the appropriate libraries to enable them to draw upon the same external resources as Oracle WebCenter Spaces. For more information about managed servers, see "Understanding Oracle Fusion Middleware Concepts" in the *Oracle Fusion Middleware Administrator's Guide*.

### 1.3.1 Oracle WebCenter Managed Servers

During Oracle WebCenter installation, the managed servers are provisioned with system libraries and ADF libraries. [Table 1–1](#) lists the managed servers and the applications that run on them.

**Table 1–1 Oracle WebCenter Managed Servers and Applications**

| Managed Server  | Application(s)              |
|---|-----------------------------|
| WLS_Spaces  | webcenter<br>webcenter-help |
| WLS_Portlets  | portalTools<br>wsrp-tools   |
| WLS_Services<br>(Discussions server and Wiki and Blog server) | owc_discussions<br>owc_wiki |

### 1.3.2 Oracle WebCenter Startup Order

When a managed server starts up, applications and libraries are started in the following order:

1. Oracle system libraries, known as the JRF libraries
2. ADF libraries
3. Instrumentation applications, such as Oracle DMS
4. Oracle Web Services Manager (wsm-pm) application
5. WebCenter applications, shown in [Table 1–1](#)

The startup order is also the order of dependency. If a dependent component does not deploy successfully, a later component may not function correctly.

WebCenter application startup is not dependent on the availability of external services such as the Discussions server, or other back-end servers. For details, see [Section 1.3.3, "Oracle WebCenter External Dependencies"](#).

### 1.3.3 Oracle WebCenter External Dependencies

WebCenter applications have several external dependencies, as listed in [Table 1–2](#). The Configuration column lists the type of information provided to Oracle WebCenter to configure or initialize the connection. The Access column lists the protocol used in run-time access of the service.

Server/service unavailability will not prevent WebCenter applications from starting up, although errors may display while the application is running. The only exception is the Oracle Metadata Repository (MDS), as WebCenter applications do not work without it. WebCenter Spaces partially works without the WebCenter repository, but only if it is a different physical database from the MDS repository.

**Table 1–2 External Resources - Access Types**

| External Server/Service               | Configuration   | Access                      |
|---------------------------------------|---|-----------------------------|
| Discussions server                    | HTTP access to discussions server administration  | SOAP/HTTP                   |
| Oracle Content Server (Documents)     | Socket connection to the Administration Server. HTTP access is required only if the Oracle Content Server must be accessed outside WebCenter. | JCR 1.0 over socket or HTTP |
| Instant Messaging and Presence server | HTTP access to instant messaging and presence server administration   | SOAP/HTTP                   |
| Mail server                           | IMAP/SMTP server  | IMAP/SMTP                   |
| Portlets                              | HTTP location of provider WSDLs   | SOAP/HTTP                   |
| Search server                         | HTTP access to search server  | HTTP                        |
| Wiki and Blog server                  | HTTP access to wiki server administration   | SOAP/HTTP                   |
| Worklist                              | HTTP access to BPEL server  | SOAP/HTTP                   |
| MDS and Schemas                       | JDBC  | JDBC                        |

Configure each of the external services independently for high availability. Oracle WebCenter provides a single point of access for external services.

- For HTTP services, direct the access URL to a load balancer, which provides access to multiple service providers on the back-end.
- For the MDS and schemas, Oracle recommends an Oracle Real Application Clusters (RAC) database as the back-end database.

### 1.3.4 Oracle WebCenter Configuration Considerations

The main configuration files for WebCenter applications are listed and described in [Table 1–3](#). Both these files are supplied within the WebCenter application deployment .EAR file.

**Table 1–3 Oracle WebCenter Configuration Files**

| Artifact                     | Purpose  |
|------------------------------|--|
| <code>adf-config.xml</code>  | Stores basic configuration for Application Development Framework (ADF) and WebCenter application settings, such as which discussions server or mail server the WebCenter application is currently using. |
| <code>connections.xml</code> | Stores basic configuration for connections to external services.   |

WebCenter applications and portlet producers both use the Oracle Metadata Services (MDS) repository to store their configuration data; both access the MDS repository as a JDBC data source within the Oracle WebLogic framework.

The MDS repository stores post deployment configuration changes for WebCenter applications and portlet producers as customizations. MDS uses the original deployed versions of `adfconfig.xml` and `connection.xml` as base documents and stores all subsequent customizations separately into MDS using a single customization layer.

When a WebCenter application starts up, customizations stored in MDS are applied to the appropriate base documents and the WebCenter application uses the merged documents (base documents with customizations) as the final set of configuration properties.

For WebCenter applications that are deployed to a server cluster, all members of a cluster read from the same location in the MDS repository.

Typically, there is no need for administrators to examine or manually change the content of base documents (or MDS customization data) for files such as `adfconfig.xml` and `connection.xml`, as Oracle provides several administration tools for post deployment configuration. If you must locate the base documents or review the information in MDS, read [Appendix A, "WebCenter Configuration"](#).

To find out more about WebCenter application configuration tools available, see [Section 1.12, "Oracle WebCenter Administration Tools"](#).

---



---

**Note:** Oracle does not recommend that you edit `adfconfig.xml` or `connection.xml` by hand (unless specifically instructed to do so) as this can lead to misconfiguration.

---



---

While WebCenter applications and portlet producers store post-deployment configuration information in MDS, configuration information for Oracle WebCenter Discussions Server and Oracle WebCenter Wiki and Blog Server is stored in the file system (see [Table 1-4](#)).

**Table 1-4 Oracle WebCenter Configuration Location**

| Application                   | Configuration Stored in MDS | Configuration Stored in the File System |
|-------------------------------|-----------------------------|---|
| WebCenter Spaces              | Yes                         | No                                      |
| Custom WebCenter applications | Yes                         | No                                      |
| Portlet producers             | Yes                         | No                                      |
| Discussions server            | No                          | Yes                                     |
| Wiki and Blog server          | No                          | Yes                                     |

The Oracle WebCenter Discussions Server stores configuration information in `DOMAIN_HOME/config/fmwconfig/servers/{SERVER_NAME}/dfw_config.xml`. This configuration information is specific to a particular instance of the discussions server.

The Oracle WebCenter Wiki and Blog Server stores configuration information in the server's deployment directory. For example, `DOMAIN_HOME/servers/SERVER_NAME`. Its configuration file, `application_config.script`, is located in `DOMAIN_HOME/WEB-INF/classes`. For example, `DOMAIN_HOME/servers/WLS_Services/stage/owc_wiki/11.1.1.1.0/owc_wiki/WEB-INF/classes`.

### 1.3.5 Oracle WebCenter State and Configuration Persistence

WebCenter applications run as J2EE applications with application state and configuration persisted to the MDS repository. User session information within the application is held locally in memory. In a cluster environment, this state is replicated to other members of the cluster.



Customizations within a portlet or service environment are persisted by that service. Out-of-the-box, Oracle portlets, any custom portlets you build, Oracle WebCenter Discussions Server, and Oracle WebCenter Wiki and Blog Server all have their own database persistence mechanisms.

### 1.3.6 Oracle WebCenter Log File Locations

Operations performed by WebCenter applications, portlet producers, discussion servers, wiki and blog servers, and so on, are logged directly to the WebLogic managed server where the application is running:

```
wls_domain_directory/servers/WLS_ServerName/logs/WLS_
ServerName.log
```

You can view the log files for each WebLogic managed server from the Oracle WebLogic Server Administration Console. To view the logs, access the Oracle WebLogic Server Administration Console `http://<admin_server_host>:<port>/console`, and click **Diagnostics-Log Files**.

You can also view and configure diagnostic logs through Fusion Middleware Control, see [Section 15.3, "Viewing and Configuring Log Information"](#).

## 1.4 Oracle WebCenter Spaces

Oracle WebCenter Spaces is a Web-based application, built using the Oracle WebCenter Framework, that offers the very latest technology for social networking, communication, collaboration, and personal productivity. Through a robust set of services and applications, WebCenter Spaces brings together everything you need to exchange ideas with others, keep track of your personal and work-related tasks, interact with your critical applications, and zero in on your own projects and interests—all within a single, integrated environment.

To help you get started, see:

- [Chapter 2, "Getting WebCenter Spaces Up and Running"](#)

For information about administering WebCenter Spaces, see:

- [Chapter 17, "Accessing WebCenter Spaces Administration Pages"](#)
- [Chapter 18, "Customizing WebCenter Spaces"](#)
- [Chapter 19, "Managing Users and Roles for WebCenter Spaces"](#)
- [Chapter 20, "Managing Pages in WebCenter Spaces"](#)
- [Chapter 21, "Making Applications Available in WebCenter Spaces"](#)
- [Chapter 22, "Managing Group Spaces in WebCenter Spaces"](#)
- [Chapter 23, "Exporting and Importing Group Spaces"](#)

## 1.5 Custom WebCenter Applications

You can develop custom WebCenter applications using JDeveloper and deploy them to a custom WebLogic Managed Server. For information about developing custom WebCenter applications, see the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

To help you get started, see:

- [Chapter 4, "Getting Custom WebCenter Applications Up and Running"](#)

- [Chapter 5, "Maintaining Custom WebCenter Applications"](#)
- [Chapter 7, "Deploying WebCenter Applications"](#)

## 1.6 Planning WebCenter Installations

Installing your WebCenter application requires a little bit of planning. Some of the questions to consider are:

- What WebCenter components will be used?
- How many users will access this deployment?
- How can I provide high availability for my WebCenter enterprise deployment?
- How can I secure WebCenter?

For more information about planning a WebCenter installation, see the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*, the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle WebCenter*, and the *Oracle Fusion Middleware High Availability Guide*.

## 1.7 Understanding the WebCenter 11g Installation

The out-of-the-box WebCenter topology is briefly described in [Section 1.3, "Oracle WebCenter Topology"](#). Specific areas of the WebCenter topology are described in the corresponding chapters, for example, security-related aspects of the WebCenter topology are described in [Chapter 14, "Managing Security"](#).

For more information about Oracle WebCenter installation and post-installation administration tasks, see the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*.

For post-installation enterprise configuration, see the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle WebCenter*.

For post-installation high availability configuration, see the *Oracle Fusion Middleware High Availability Guide*.

For post-installation security configuration, see [Chapter 14, "Managing Security"](#).

## 1.8 Understanding Administrative Operations, Roles, and Tools

Oracle WebCenter provides several different tools with which to deploy, configure, start and stop, and maintain Oracle WebCenter applications. All these tools are described in [Section 1.12, "Oracle WebCenter Administration Tools"](#).

Your ability to perform WebCenter administration tasks depends on which Oracle WebLogic Server role you are assigned—Admin, Operator, or Monitor. [Table 1–5](#) lists the Oracle WebLogic Server roles needed for common operations. These roles apply whether the operations are performed through Fusion Middleware Control, WLST commands, or the WebLogic Server Administration Console.

**Table 1–5 WebCenter Operations and Oracle WebLogic Server Roles**

| Operation                  | Admin Role | Operator Role | Monitor Role |
|----------------------------|------------|---------------|--------------|
| All WebCenter applications |            |               |              |
| Start and stop             | Yes        | Yes           | No           |

**Table 1–5 (Cont.) WebCenter Operations and Oracle WebLogic Server Roles**

| <b>Operation</b>                           | <b>Admin Role</b> | <b>Operator Role</b> | <b>Monitor Role</b> |
|--|-------------------|----------------------|---------------------|
| View performance metrics                   | Yes               | Yes                  | Yes                 |
| View log information                       | Yes               | Yes                  | Yes                 |
| Configure log files                        | Yes               | Yes                  | Yes                 |
| View configuration                         | Yes               | Yes                  | Yes                 |
| Configure new connections                  | Yes               | Yes                  | No                  |
| Edit connections                           | Yes               | Yes                  | No                  |
| Delete connections                         | Yes               | Yes                  | No                  |
| Deploy applications                        | Yes               | No                   | No                  |
| Configure security                         | Yes               | No                   | No                  |
| View security (application roles/policies) | Yes               | Yes                  | Yes                 |
| <b>WebCenter Spaces only</b>               |                   |                      |                     |
| Export WebCenter Spaces                    | Yes               | No                   | No                  |
| Import WebCenter Spaces                    | Yes               | No                   | No                  |

Table 1–6 summarizes which tools can be used to perform various administrative operations relating to WebCenter applications.

**Table 1–6 WebCenter Operations and Administration Tools**

| <b>Operation</b>                  | <b>Fusion Middleware Control</b> | <b>WLST Commands</b> | <b>WebLogic Server Admin Console</b> | <b>WebCenter Spaces Admin</b> |
|-----------------------------------|----------------------------------|----------------------|--------------------------------------|-------------------------------|
| <b>All WebCenter applications</b> |                                  |                      |                                      |                               |
| Start and stop                    | Yes                              | Yes                  | Yes                                  | No                            |
| View performance metrics          | Yes                              | No                   | No                                   | No                            |
| View log information              | Yes                              | No                   | No                                   | No                            |
| Configure log files               | Yes                              | No                   | No                                   | No                            |
| View configuration                | Yes                              | Yes                  | No                                   | No                            |
| Configure new connections         | Yes                              | Yes                  | No                                   | No                            |
| Edit connections                  | Yes                              | Yes                  | No                                   | No                            |
| Delete connections                | Yes                              | Yes                  | No                                   | No                            |
| Deploy applications               | Yes                              | Yes                  | Yes                                  | No                            |
| Configure security                | Yes                              | Yes                  | Yes                                  | No                            |
| <b>WebCenter Spaces only</b>      |                                  |                      |                                      |                               |
| Configure workflows               | Yes                              | Yes                  | No                                   | No                            |
| Export WebCenter Spaces           | Yes                              | Yes                  | No                                   | No                            |
| Import WebCenter Spaces           | Yes                              | Yes                  | No                                   | No                            |
| Customize WebCenter Spaces        | No                               | No                   | No                                   | Yes                           |

**Table 1–6 (Cont.) WebCenter Operations and Administration Tools**

| Operation                          | Fusion Middleware Control | WLST Commands | WebLogic Server Admin Console | WebCenter Spaces Admin |
|------------------------------------|---------------------------|---------------|-------------------------------|------------------------|
| Manage application users and roles | No                        | No            | No                            | Yes                    |
| Manage pages                       | No                        | No            | No                            | Yes                    |
| Manage group spaces                | No                        | No            | No                            | Yes                    |
| Export group spaces                | No                        | No            | No                            | Yes                    |
| Import group spaces                | No                        | No            | No                            | Yes                    |

## 1.9 Performance Monitoring and Diagnostics

Performance monitoring helps administrators identify issues and performance bottlenecks in their environment. [Chapter 15, "Monitoring Oracle WebCenter Performance"](#) describes the range of performance metrics available for WebCenter applications and how to monitor them using Fusion Middleware Control. It also describes how to troubleshoot issues by analyzing information that is recorded in WebCenter diagnostic log files.

## 1.10 WebCenter Application Deployment

[Chapter 7, "Deploying WebCenter Applications"](#) provides instructions for deploying, redeploying, and undeploying custom WebCenter applications from an .EAR file created with Oracle JDeveloper.

[Section 12.8, "Deploying Portlet Producer Applications"](#) provides instructions for deploying WSRP and PDK-Java portlet producer applications.

---

**Note:** Oracle WebCenter Spaces is deployed during installation (it cannot be deployed as an .EAR file). See "Installing Oracle WebCenter" in the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*.

---

## 1.11 Data Migration, Backup, and Recovery

Oracle WebCenter stores data related to its configuration and content for the various feature areas in a several locations. To facilitate disaster recovery and the full production lifecycle from development through staging and production, WebCenter provides a set of utilities that enable you to back up this data, and move the data between WebCenter applications in staging and production environments.

[Chapter 16, "Managing Export, Import, Backup, and Recovery of WebCenter"](#) describes the backup, import, and export capabilities and tools available for these tasks.

## 1.12 Oracle WebCenter Administration Tools

Oracle offers the following tools for managing Oracle WebCenter:

- [Oracle Enterprise Manager Fusion Middleware Control Console](#)
- [Oracle WebLogic Server Administration Console](#)
- [Oracle WebLogic Scripting Tool \(WLST\)](#)

All of these administration tools apply to all WebCenter applications. For managing WebCenter Spaces specifically, you can also use:

- [WebCenter Spaces Administration Pages](#)

Administrators should use these tools, rather than edit configuration files, to perform administrative tasks, unless a specific procedure requires you to edit a file. Editing a file may cause the settings to be inconsistent and generate problems. See also, [Appendix A, "WebCenter Configuration"](#).

### 1.12.1 Oracle Enterprise Manager Fusion Middleware Control Console

Oracle Enterprise Manager Fusion Middleware Control Console is a browser-based management application that is deployed when you install Oracle WebCenter. From Fusion Middleware Control Console, you can monitor and administer a *farm* (such as one containing Oracle WebCenter and WebCenter applications).

Fusion Middleware Control organizes a wide variety of performance data and administrative functions into distinct, web-based home pages. These home pages make it easy to locate the most important monitoring data and the most commonly used administrative functions for any WebCenter component—all from your web browser. For general information about the Fusion Middleware Control Console, see "Getting Started Using Oracle Enterprise Manager Fusion Middleware Control" in the *Oracle Fusion Middleware Administrator's Guide*.

Fusion Middleware Control is the primary management tool for Oracle WebCenter and can be used to:

- Deploy, undeploy, and re-deploy WebCenter applications
- Configure back-end services
- Configure security management
- Control process lifecycle
- Access log files and manage log configuration
- Manage data migration
- Monitor performance
- Diagnose run-time problems
- Manage related components, such as the parent Managed Server, MDS, portlet producers, and so on

#### 1.12.1.1 Displaying Fusion Middleware Control Console

For information about starting Fusion Middleware Control, see [Section 6.1, "Displaying Fusion Middleware Control Console"](#).

### 1.12.2 Oracle WebLogic Server Administration Console

The Oracle WebLogic Server Administration Console is a browser-based, graphical user interface that you use to manage a WebLogic Server domain.

The Administration Server hosts the Administration Console, which is a Web application accessible from any supported Web browser with network access to the Administration Server Managed Servers host applications.

Use the Administration Console to:

- Configure, start, and stop WebLogic Server instances
- Configure WebLogic Server clusters
- Configure WebLogic Server services, such as database connectivity (JDBC) and messaging (JMS)
- Configure security parameters, including creating and managing users, groups, and roles
- Configure and deploy your applications
- Monitor server and application performance
- View server and domain log files
- View application deployment descriptors
- Edit selected run-time application deployment descriptor elements

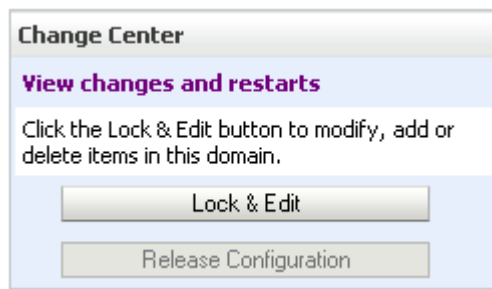
For more information about the Oracle WebLogic Server Administration Console, see "Displaying the Oracle WebLogic Server Administration Console" in the *Oracle Fusion Middleware Administrator's Guide*.

### Locking Domain Configuration

In a production environment, you must lock configuration settings for a domain before making any configuration changes. Navigate to the Administration Console's Change Center (Figure 1–3), and click **Lock & Edit**.

Once configuration updates are complete, release the changes by clicking **Release Configuration**.

**Figure 1–3 Change Center in Oracle WebLogic Server Administration Console**



### 1.12.3 Oracle WebLogic Scripting Tool (WLST)

Oracle provides the WebLogic Scripting Tool (WLST) to manage Oracle Fusion Middleware components, such as Oracle WebCenter, from the command line.

WLST is a complete, command-line scripting environment for managing Oracle WebLogic Server domains, based on the Java scripting interpreter, Jython. In addition to supporting standard Jython features such as local variables, conditional variables, and flow control statements, WLST provides a set of scripting functions (commands) that are specific to Oracle WebLogic Server. You can extend the WebLogic scripting language to suit your needs by following the Jython language syntax.

Oracle WebCenter offers WLST commands for managing WebCenter application connections (to content repositories, portlet producers, external applications, and other back-end services), and also for exporting and importing the WebCenter Spaces

application. All Oracle WebCenter WLST commands are described in "Oracle WebCenter Custom WLST Commands" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

### 1.12.3.1 Running Oracle WebLogic Scripting Tool (WLST) Commands

To run WLST from the command line:

1. Navigate to the directory `WC_HOME/common/bin`.
2. From the command line, enter the command:

```
wlst.sh
```

For example:

```
WC_HOME/common/bin/wlst.sh
```

3. At the WLST command prompt, enter the following command to connect to the Administration Server for Oracle WebCenter:

```
wls:/offline>connect('<user_name>','<password>', '<host_name>:<port_number>')
```

where

- `<user_name>` is the username of the operator who is connecting to the Administration Server
- `<password>` is the password of the operator who is connecting to the Administration Server
- `<host_name>` is the host name of the Administration Server
- `<port_number>` is the port number of the Administration Server

For example:

```
connect('weblogic','weblogic','myhost.example.com:7001')
```

For help for this command, type `help('connect')` at the WLST command prompt.

---

**Note:** If SSL is enabled, you must edit the `wlst.sh` file and append the following to `JVM_ARGS`:

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

or `setenv CONFIG_JVM_ARGS`

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

---

4. Once connected to the Administration Server you can run any Oracle WebCenter or generic WLST command.

For a complete list, see "Oracle WebCenter Custom WLST Commands" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

## 1.12.4 WebCenter Spaces Administration Pages

WebCenter Spaces provides several administration pages of its own. WebCenter Spaces Administration appears only to users who have logged in to the application using an administrator user name and password. See also, [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).

WebCenter Spaces administration pages allow you to:

- Customize WebCenter Spaces
- Manage users and roles
- Manage services settings for WebCenter Spaces
- Manage group spaces and group space templates
- Create and manage business role pages
- Manage personal pages
- Export and import group spaces

For more details, see [Section 17, "Accessing WebCenter Spaces Administration Pages"](#).



# Part II

---

## Getting Started With Oracle WebCenter Administration

This part of the Administrator's Guide provides checklists to help you get started with Oracle WebCenter administration.

Part II contains the following chapters:

- [Chapter 2, "Getting WebCenter Spaces Up and Running"](#)
- [Chapter 3, "Maintaining WebCenter Spaces"](#)
- [Chapter 4, "Getting Custom WebCenter Applications Up and Running"](#)
- [Chapter 5, "Maintaining Custom WebCenter Applications"](#)



---

---

# Getting WebCenter Spaces Up and Running

Getting WebCenter Spaces up and running and ready for use requires input from both the *Fusion Middleware administrator* and the *WebCenter Spaces administrator*. This chapter outlines the roles and responsibilities of each administrator who may, in some cases, be the same person.

The chapter also outlines what must be done, after installation, to get WebCenter Spaces up and running. Some roadmaps are provided to guide you through this process.

This chapter includes the following sections:

- [Role of the Fusion Middleware Administrator](#)
- [Role of the WebCenter Spaces Administrator](#)
- [Installing WebCenter Spaces](#)
- [Setting Up WebCenter Spaces for the First Time \(Roadmap\)](#)
- [Customizing WebCenter Spaces for the First Time \(Roadmap\)](#)

## Audience

The content of this chapter is intended for Fusion Middleware administrators responsible for WebCenter Spaces (users granted the `Admin` role through the Oracle WebLogic Server Administration Console) and WebCenter Spaces administrators (users granted the `Administrator` role through WebCenter Spaces Administration).

---

---

**Note:** Administrators working with custom WebCenter applications developed using Oracle WebCenter Framework, should refer to [Chapter 4, "Getting Custom WebCenter Applications Up and Running"](#).

---

---

## 2.1 Role of the Fusion Middleware Administrator

Oracle Fusion Middleware provides a single administrative role with *complete* administrative capabilities—the `Admin` role. Fusion Middleware administrators with this role can perform the complete range of security-sensitive administrative duties, as well as all installation, configuration, and audit tasks. This administrator is also responsible for setting up and configuring WebCenter Spaces immediately after installation, and performing on-going administrative tasks for WebCenter Spaces and other Oracle WebCenter components. Throughout this document we refer to this administrator as the *Fusion Middleware administrator*.

During installation, a single Fusion Middleware administrator account is created named `weblogic`. The password is the one provided during installation.

Use this administrator account to log in to the Fusion Middleware Control Console and WebCenter Spaces, and assign administrative privileges to other users:

- **Fusion Middleware Control** - Add one more users to the `Administrator` group using the Oracle WebLogic Administration Console or Oracle WebLogic Scripting Tool (WLST). For details, see "Administrative Users and Roles" in *Oracle Fusion Middleware Security Guide*.

Oracle WebLogic Server provides two other roles, in addition to the `Admin` role, namely `Operator` and `Monitor`. To find out more about these role, see [Table 1–5, "WebCenter Operations and Oracle WebLogic Server Roles"](#) in [Section 1.8, "Understanding Administrative Operations, Roles, and Tools"](#).

- **WebCenter Spaces** - Assign one more users the `Administrator` role through WebCenter Spaces Administration. For details, see [Giving a User Administrative Privileges](#).

To find out what other tasks a Fusion Middleware administrator must do to get WebCenter Spaces up and running, follow the [Roadmap - Customizing WebCenter Spaces for the First Time](#).

---

---

**Note:** The Fusion Middleware administrator is also responsible for all on-going administrative tasks, for details see [Section 3.3, "System Administration for WebCenter Spaces \(Roadmap\)"](#).

---

---

## 2.2 Role of the WebCenter Spaces Administrator

WebCenter Spaces administrators have the highest application privileges within the WebCenter Spaces application itself. This administrator can view and customize every aspect of the WebCenter Spaces application and is responsible for customizing WebCenter Spaces out-of-the-box and maintaining the application once it is in use.

Out-of-the-box, the default Fusion Middleware administrator (`weblogic`) is the only user assigned to the WebCenter Spaces `Administrator` role. The password is the one provided during installation. Use this administrator account to log in to WebCenter Spaces, and assign additional users the `Administrator` role. For details, see [Giving a User Administrative Privileges](#).

To find out what a WebCenter Spaces administrator must do to customize WebCenter Spaces out-of-the-box, follow the [Roadmap - Customizing WebCenter Spaces for the First Time](#).

---

---

**Note:** The WebCenter Spaces administrator is also responsible for all on-going administrative tasks, for details see [Section 3.4, "Application Administration for WebCenter Spaces \(Roadmap\)"](#).

---

---

## 2.3 Installing WebCenter Spaces

WebCenter Spaces installation is described in the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*.

## 2.4 Setting Up WebCenter Spaces for the First Time (Roadmap)

The roadmap in [Table 2–1](#) outlines the tasks that a Fusion Middleware administrator must perform to get a WebCenter Spaces up and running.

**Table 2–1 Roadmap - Setting Up WebCenter Spaces for the First Time**

| Step   | Documentation  | Role                    |
|--|--|-------------------------|
| <b>Step 1 - Verify your Oracle WebCenter Spaces installation</b> | <p>Install WebCenter Spaces, start the managed server, log in to the application with default credentials, and assign administration privileges to one or more users:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">Installing WebCenter Spaces</a></li> <li>▪ <a href="#">Starting Node Manager</a></li> <li>▪ <a href="#">Starting and Stopping Managed Servers for WebCenter Application Deployments</a></li> <li>▪ <a href="#">Logging into WebCenter Spaces as an Administrator</a></li> <li>▪ <a href="#">Giving a User Administrative Privileges</a></li> </ul> <p>Tip: WebCenter Spaces URL is<br/> <a href="http://&lt;host&gt;:&lt;port&gt;/webcenter/spaces">http://&lt;host&gt;:&lt;port&gt;/webcenter/spaces</a></p> <p>If the default administrator was changed at install time, you must grant that user WebCenter Spaces administrative privileges before logging in to WebCenter Spaces. See "<a href="#">Granting the WebCenter Administrator Role to a WebCenter Spaces User</a>".</p> | Fusion Middleware Admin |
| <b>Step 2 - Launch Fusion Middleware Control</b>                 | <p>Launch Fusion Middleware Control Console, a Web-based management tool for WebCenter Spaces:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">Displaying Fusion Middleware Control Console</a></li> <li>▪ <a href="#">Navigating to the Home Page for WebCenter Spaces</a></li> </ul> <p>Tip: Fusion Middleware Control Console URL is<br/> <a href="http://&lt;host&gt;:&lt;port&gt;/em">http://&lt;host&gt;:&lt;port&gt;/em</a></p> <p>Learn about the command-line administration tool WLST. See "<a href="#">Oracle WebLogic Scripting Tool (WLST)</a>".</p>   | Fusion Middleware Admin |
| <b>Step 3 - Configure WebCenter Spaces workflows</b>             | <p>Connect the application to the BPEL server where WebCenter Spaces workflows are installed:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">Back-End Requirements for WebCenter Spaces Workflows</a></li> <li>▪ <a href="#">Specifying the BPEL Server Hosting WebCenter Spaces Workflows</a></li> </ul>  | Fusion Middleware Admin |
| <b>Step 4 - Connect back-end services</b>                        | <p>Configure back-end services for WebCenter Spaces through Fusion Middleware Control Console. See:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">Content Repositories</a></li> <li>▪ <a href="#">Mail Servers</a></li> <li>▪ <a href="#">BPEL Servers</a></li> <li>▪ <a href="#">Collaboration Services</a></li> <li>▪ <a href="#">Secure Enterprise Search</a></li> </ul>   | Fusion Middleware Admin |
|  | <ul style="list-style-type: none"> <li>▪ <a href="#">Managing Content Repositories</a></li> <li>▪ <a href="#">Setting Up Connections for the Mail Service</a></li> <li>▪ <a href="#">Setting Up Worklist Connections</a></li> <li>▪ <a href="#">Setting Up Connections for the Discussions and Announcements Services</a></li> <li>▪ <a href="#">Setting Up Connections for the Instant Messaging and Presence Service</a></li> <li>▪ <a href="#">Setting Up the Server for Wiki and Blog Services</a></li> <li>▪ <a href="#">Setting Up Connections for the Search Service</a></li> </ul>   |                         |

**Table 2–1 (Cont.) Roadmap - Setting Up WebCenter Spaces for the First Time**

| Step  | Documentation  | Role                    |
|---|--|-------------------------|
| <ul style="list-style-type: none"> <li>Wiki and Blog Services</li> </ul>                            | <ul style="list-style-type: none"> <li><a href="#">Setting Up the Server for Wiki and Blog Services</a></li> </ul>   |                         |
| <ul style="list-style-type: none"> <li>Group Space Events, Links, Lists, Notes, and Tags</li> </ul> | <ul style="list-style-type: none"> <li>No additional set up required. The WebCenter repository and MDS repository required for these services are configured out-of-the-box.</li> </ul>  |                         |
| <b>Step 5 - Connect external applications and portlet producers</b>                                 | Configure external applications and portlet producers for WebCenter Spaces. See:   | Fusion Middleware Admin |
| <ul style="list-style-type: none"> <li>External Applications</li> <li>Portlet Producers</li> </ul>  | <ul style="list-style-type: none"> <li><a href="#">Managing External Applications</a></li> <li><a href="#">Registering WSRP Producers</a></li> <li><a href="#">Registering Oracle PDK-Java Producers</a></li> </ul>  |                         |
| <b>Step 6 - Connect back-end servers to the same identity store as WebCenter Spaces</b>             | <p>Ensure that back-end servers, supporting Wikis and Blogs, Discussions and Announcements, Presence, and Oracle Content Server, share the same identity store as WebCenter Spaces:</p> <ul style="list-style-type: none"> <li><a href="#">Configuring the Identity Store</a></li> </ul> <p>See also <i>Oracle Fusion Middleware Security Guide</i>.</p>   | Fusion Middleware Admin |
| <b>Step 7 - Secure communication with WebCenter Spaces</b>  | <p>Configure secure communication:</p> <ul style="list-style-type: none"> <li><a href="#">Configuring WebCenter Applications and Components to Use SSL</a></li> <li><a href="#">Configuring WS-Security</a></li> <li><a href="#">Configuring a WebCenter Application to Use Single Sign-On</a></li> </ul> <p>See also <i>Oracle Fusion Middleware Security Guide</i>.</p>                            | Fusion Middleware Admin |
| <b>Step 8 - Restart the managed server and WebCenter Spaces</b>                                     | <p>Restart the managed server on which WebCenter Spaces is deployed to effect configuration changes, and then login to WebCenter Spaces with administrative privileges:</p> <ul style="list-style-type: none"> <li><a href="#">Starting and Stopping Managed Servers for WebCenter Application Deployments</a></li> <li><a href="#">Logging into WebCenter Spaces as an Administrator</a></li> </ul> | Fusion Middleware Admin |
| <b>Step 9 - Verify your WebCenter Spaces configuration</b>  | <p>Verify WebCenter Spaces configuration: identity store, services, applications, and so on.</p> <ul style="list-style-type: none"> <li><a href="#">Logging into WebCenter Spaces as an Administrator</a></li> </ul> <p>Tip: WebCenter Spaces URL is<br/> <code>http://&lt;host&gt;:&lt;port&gt;/webcenter/spaces</code></p>   | Fusion Middleware Admin |
| <b>Step 10 - Customize WebCenter Spaces and grant application roles</b>                             | <p>The WebCenter Spaces administrator is responsible for WebCenter Spaces customizations and user role assignments:</p> <ul style="list-style-type: none"> <li><a href="#">Customizing WebCenter Spaces for the First Time (Roadmap)</a></li> </ul>  | WebCenter Spaces Admin  |

## 2.5 Customizing WebCenter Spaces for the First Time (Roadmap)

The roadmap in [Table 2–2](#) outlines the tasks that a WebCenter Spaces administrator might perform to customize WebCenter Spaces for a new target audience.

**Table 2–2 Roadmap - Customizing WebCenter Spaces for the First Time**

| <b>Step</b>   | <b>Documentation</b>   | <b>Role</b>            |
|---|--|------------------------|
| <b>Step 1 - Log in to WebCenter Spaces</b>                                | <p>Login to WebCenter Spaces with administrative privileges and access the administration pages:</p> <ul style="list-style-type: none"> <li>■ <a href="#">Logging into WebCenter Spaces as an Administrator</a></li> </ul> <p>Tip: WebCenter Spaces URL is<br/>http://&lt;host&gt;:&lt;port&gt;/webcenter/spaces</p>   | WebCenter Spaces Admin |
| <b>Step 2 - Customize WebCenter Spaces</b>                                | <p>Customize WebCenter Spaces to suit your audience. Choose a name and logo for your application, apply a corporate brand, set language options, and more:</p> <ul style="list-style-type: none"> <li>■ <a href="#">Naming Your WebCenter</a></li> <li>■ <a href="#">Customizing the Online Help Link</a></li> <li>■ <a href="#">Choosing the Default Display Language</a></li> <li>■ <a href="#">Applying Look and Feel using Skins</a></li> <li>■ <a href="#">Customizing Copyright and Privacy Statements</a></li> <li>■ ... for more options, see <a href="#">Chapter 18, "Customizing WebCenter Spaces"</a>.</li> </ul> | WebCenter Spaces Admin |
| <b>Step 3 - Determine self-registration policy</b>                        | <p>Establish your policy regarding new user registration. Allow users outside of the WebCenter Spaces community by to self-register on an invitation-only basis or extend self-registration to the public:</p> <ul style="list-style-type: none"> <li>■ <a href="#">Enabling Self-Registration By Invitation-Only</a></li> <li>■ <a href="#">Enabling Anyone to Self-Register</a></li> </ul>   | WebCenter Spaces Admin |
| <b>Step 4 - Plan the public user experience</b>                           | <p>First impressions are extremely important. Determine the content displayed on your Welcome page and the appearance of WebCenter Spaces before users login:</p> <ul style="list-style-type: none"> <li>■ <a href="#">Customizing the Public Welcome Page</a></li> <li>■ <a href="#">Customizing the Login Page</a></li> <li>■ <a href="#">Customizing the Self-Registration Page</a></li> <li>■ <a href="#">Choosing the Default Display Language</a></li> <li>■ <a href="#">Granting Permissions to the Public-User</a></li> </ul>  | WebCenter Spaces Admin |
| <b>Step 5 - Create roles and delegate responsibilities to other users</b> | <p>Create roles to characterize groups of WebCenter users and determine what they can see and do in WebCenter Spaces. Manage and assign roles for any user in the identity store:</p> <ul style="list-style-type: none"> <li>■ <a href="#">Understanding Users, Roles, and Permissions</a></li> <li>■ <a href="#">Assigning Users to Roles</a></li> <li>■ <a href="#">Defining Application Roles</a></li> <li>■ <a href="#">Giving a User Administrative Privileges</a></li> <li>■ <a href="#">Modifying Application Role Permissions</a></li> </ul>   | WebCenter Spaces Admin |

**Table 2–2 (Cont.) Roadmap - Customizing WebCenter Spaces for the First Time**

| <b>Step</b>  | <b>Documentation</b>  | <b>Role</b>            |
|--|---|------------------------|
| <b>Step 6 - Customize personal spaces</b>                      | <p>Design a default personal space for your WebCenter users. Give them instant access to important information and applications relevant to their roles:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">Setting Up a Default Look and Feel for Personal Pages</a></li> <li>▪ <a href="#">Creating a Business Role Page</a></li> </ul> <p>Encourage or enforce a consistent look and feel through default page schemes and default page templates:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">Setting Up a Default Look and Feel for Personal Pages</a></li> </ul> | WebCenter Spaces Admin |
| <b>Step 7 - Set up discussion forums and announcements</b>     | <p>Configure default options for discussion forums and announcements:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">Setting Discussion Forum Options</a></li> </ul>  | WebCenter Spaces Admin |
| <b>Step 8 - Set up personal profiles</b>                       | <p>Configure personal profiles, and whether users can edit their profile data and their password in WebCenter Spaces:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">Managing Personal Profiles</a></li> </ul>  | WebCenter Spaces Admin |
| <b>Step 9 - Provide group spaces and group space templates</b> | <p>In WebCenter, users can create and manage group spaces without centralized administration. Give them a head-start by creating templates for the types of group spaces they are likely to build:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">Building Group Spaces</a></li> <li>▪ <a href="#">Creating Group Space Templates</a></li> </ul>  | WebCenter Spaces Admin |
| <b>Step 10 - Customize the Sidebar</b>                         | <p>Give users quick access to frequently used applications and collaboration services such as mail, worklist assignments, and personal contacts. Display, hide, reorganize, and lock the content of everyone's Personal Sidebar:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">Hiding and Showing Task Flows in the Sidebar</a></li> <li>▪ <a href="#">Locking Sidebar Content</a></li> </ul>  | WebCenter Spaces Admin |
| <b>Step 11 - Organize the applications pane</b>                | <p>Make WebCenter the single place a user needs to go. Allow users direct access to applications outside WebCenter Spaces that require an HTML form-based login. Expose key external applications in everyone's Personal Sidebar:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">Making an Application Available to WebCenter Users</a></li> <li>▪ <a href="#">Arranging the Applications List</a></li> <li>▪ <a href="#">Locking Applications Displayed in the Applications Pane</a></li> </ul>  | WebCenter Spaces Admin |



---

---

## Maintaining WebCenter Spaces

Keeping the WebCenter Spaces application up and running requires input from both the *Fusion Middleware administrator* and the *WebCenter Spaces administrator*. This chapter outlines the roles and responsibilities of each administrator who may, in some cases, be the same person.

Some roadmaps are also provided to help guide you through the process.

This chapter includes the following sections:

- [Role of the Fusion Middleware Administrator](#)
- [Role of the WebCenter Spaces Administrator](#)
- [System Administration for WebCenter Spaces \(Roadmap\)](#)
- [Application Administration for WebCenter Spaces \(Roadmap\)](#)

### Audience

The content of this chapter is intended for Fusion Middleware administrators responsible for WebCenter Spaces (users granted the `Admin` role through the Oracle WebLogic Server Administration Console) and WebCenter Spaces administrators (users granted the `Administrator` role through WebCenter Spaces Administration).

---

---

**Note:** Administrators maintaining custom WebCenter applications should refer to [Chapter 5, "Maintaining Custom WebCenter Applications"](#).

---

---

### 3.1 Role of the Fusion Middleware Administrator

Oracle Fusion Middleware provides a single administrative role with complete administrative capabilities—the `Admin` role. Fusion Middleware administrator can perform the complete range of security-sensitive administrative duties, as well as all installation, configuration, and audit tasks. This administrator is also responsible for setting up and configuring WebCenter Spaces immediately after installation, and performing on-going administrative tasks for WebCenter Spaces and other Oracle WebCenter components. Throughout this document we refer to this administrator as the *Fusion Middleware administrator*.

A single Fusion Middleware administrator account (`weblogic` by default) is set up when Fusion Middleware is installed. The password is the one you provided during installation.

To find out what on-going administrative tasks a Fusion Middleware administrator is expected to perform in relation to WebCenter Spaces, follow the [Roadmap - Administering and Monitoring WebCenter Spaces](#).

---

**Note:** The Fusion Middleware administrator is also responsible for getting WebCenter Spaces up and running out-of-the-box, for details see [Section 2.4, "Setting Up WebCenter Spaces for the First Time \(Roadmap\)"](#).

---

## 3.2 Role of the WebCenter Spaces Administrator

WebCenter Spaces administrators have the highest application privileges within the WebCenter Spaces application itself. This administrator can view and customize every aspect of the WebCenter Spaces application and is responsible for customizing WebCenter Spaces out-of-the-box and maintaining the application after it is in use.

Out-of-the-box, the default Fusion Middleware administrator (`weblogic`) is the only user assigned to the WebCenter Spaces Administrator role. The password is the one provided during installation.

To find out what on-going administrative tasks a WebCenter Spaces administrator is expected to perform in relation to WebCenter Spaces, follow the [Roadmap - Keeping WebCenter Spaces Up and Running](#).

---

**Note:** The WebCenter Spaces administrator is also responsible for customizing WebCenter Spaces out-of-the-box, for details see [Section 2.5, "Customizing WebCenter Spaces for the First Time \(Roadmap\)"](#).

---

## 3.3 System Administration for WebCenter Spaces (Roadmap)

The roadmap in [Table 3–1](#) outlines typical tasks that a Fusion Middleware administrator might perform to keep WebCenter Spaces up and running.

**Table 3–1 Roadmap - Administering and Monitoring WebCenter Spaces**

| Step  | Documentation  | Role                    |
|---|--|-------------------------|
| <b>Step 1 - Stop and start the managed server</b> | Restart the managed server on which WebCenter Spaces is deployed to effect configuration changes or for routine maintenance: <ul style="list-style-type: none"> <li>▪ <a href="#">Starting and Stopping Managed Servers for WebCenter Application Deployments</a></li> </ul> Tip: The managed server for WebCenter Spaces is named <code>WLS_Spaces</code> . | Fusion Middleware Admin |
| <b>Step 2 - View and manage log files</b>         | Identify and diagnose problems through log files. WebCenter Spaces logs record all types of events, including start up and shutdown information, errors, warnings, and other information: <ul style="list-style-type: none"> <li>▪ <a href="#">Viewing and Configuring Log Information</a></li> </ul>  | Fusion Middleware Admin |

**Table 3–1 (Cont.) Roadmap - Administering and Monitoring WebCenter Spaces**

| <b>Step</b>  | <b>Documentation</b>  | <b>Role</b>             |
|--|---|-------------------------|
| <b>Step 3 - Monitor performance</b>                                | Analyze the performance of WebCenter Spaces and monitor its current status through Fusion Middleware Control Console: <ul style="list-style-type: none"> <li>Viewing Performance Information</li> <li>Monitoring WebCenter Spaces</li> </ul> <p>Fusion Middleware administrators granted one of these roles can view metrics: Admin, Operator, Monitor. To find out more, see in "Understanding Administrative Operations, Roles, and Tools".</p>   | Fusion Middleware Admin |
| <b>Step 4 - Tune application properties</b>                        | Reconfigure application properties: <ul style="list-style-type: none"> <li>Tuning Environment Configuration</li> <li>Tuning WebCenter Application Configuration</li> <li>Tuning Back-End Component Configuration</li> </ul>   | Fusion Middleware Admin |
| <b>Step 3 - Stop and start WebCenter Spaces</b>                    | Fusion Middleware administrators may shut down WebCenter Spaces for maintenance purposes and then restart the application: <ul style="list-style-type: none"> <li>Starting WebCenter Spaces Using Fusion Middleware Control</li> <li>Stopping WebCenter Spaces Using Fusion Middleware Control</li> </ul>   | Fusion Middleware Admin |
| <b>Step 4 - Modify back-end services</b>                           | Add, modify, and delete connections through Fusion Middleware Control Console. See: <ul style="list-style-type: none"> <li>Content Repositories <ul style="list-style-type: none"> <li>Managing Content Repositories</li> </ul> </li> <li>Mail Servers <ul style="list-style-type: none"> <li>Setting Up Connections for the Mail Service</li> </ul> </li> <li>BPEL Servers <ul style="list-style-type: none"> <li>Setting Up Worklist Connections</li> </ul> </li> <li>Collaboration Services <ul style="list-style-type: none"> <li>Setting Up Connections for the Discussions and Announcements Services</li> <li>Setting Up Connections for the Instant Messaging and Presence Service</li> <li>Setting Up the Server for Wiki and Blog Services</li> </ul> </li> <li>Secure Enterprise Search <ul style="list-style-type: none"> <li>Setting Up Connections for the Search Service</li> </ul> </li> <li>Wiki and Blog Services <ul style="list-style-type: none"> <li>Setting Up the Server for Wiki and Blog Services</li> </ul> </li> <li>Group Space Events, Links, Lists, Notes, and Tags <ul style="list-style-type: none"> <li>Setting Up the WebCenter Repository</li> <li>Setting Up the MDS Repository</li> </ul> </li> </ul> | Fusion Middleware Admin |
| <b>Step 4 - Modify external applications and portlet producers</b> | Add, modify, and delete connections through Fusion Middleware Control Console. See: <ul style="list-style-type: none"> <li>External Applications <ul style="list-style-type: none"> <li>Managing External Applications</li> </ul> </li> <li>Portlet Producers <ul style="list-style-type: none"> <li>Registering WSRP Producers</li> <li>Registering Oracle PDK-Java Producers</li> </ul> </li> </ul>   | Fusion Middleware Admin |

**Table 3–1 (Cont.) Roadmap - Administering and Monitoring WebCenter Spaces**

| Step   | Documentation  | Role                          |
|--|--|-------------------------------|
| <b>Step 5 - Configure SSL communication</b>                | Configure secure communication: <ul style="list-style-type: none"> <li>■ <a href="#">Configuring WebCenter Applications and Components to Use SSL</a></li> <li>■ <a href="#">Configuring WS-Security</a></li> <li>■ <a href="#">Configuring a WebCenter Application to Use Single Sign-On</a></li> </ul> See also <i>Oracle Fusion Middleware Security Guide</i> .   | Fusion<br>Middleware<br>Admin |
| <b>Step 6 - Reconfigure identity store or policy store</b> | Reconfigure your identity or policy stores: <ul style="list-style-type: none"> <li>■ <a href="#">Configuring the Identity Store</a></li> <li>■ <a href="#">Configuring the Policy and Credential Store to Use OID</a></li> </ul> See also <i>Oracle Fusion Middleware Security Guide</i> .   | Fusion<br>Middleware<br>Admin |
| <b>Step 7 - Reconfigure WebCenter repository</b>           | Reconfigure the WebCenter repository: <ul style="list-style-type: none"> <li>■ <a href="#">Setting Up the WebCenter Repository</a></li> </ul>  | Fusion<br>Middleware<br>Admin |
| <b>Step 8 - Reconfigure MDS repository</b>                 | Reconfigure the application's MDS repository: <ul style="list-style-type: none"> <li>■ <a href="#">Setting Up the MDS Repository</a></li> </ul> See also <i>Oracle Fusion Middleware Administrator's Guide</i> : <ul style="list-style-type: none"> <li>■ <a href="#">Managing the MDS Repository</a></li> <li>■ <a href="#">Configuring an Application to Use a Different MDS Repository or Partition</a></li> <li>■ <a href="#">Moving Metadata from a Test System to a Production System</a></li> </ul> | Fusion<br>Middleware<br>Admin |
| <b>Step 9 - Reconfigure WebCenter Spaces workflows</b>     | Install WebCenter Spaces workflows on a different BPEL server and reconfigure the connection: <ul style="list-style-type: none"> <li>■ <a href="#">Installing WebCenter Spaces Workflows</a></li> <li>■ <a href="#">Specifying the BPEL Server Hosting WebCenter Spaces Workflows</a></li> </ul>   | Fusion<br>Middleware<br>Admin |
| <b>Step 10 - Export WebCenter Spaces</b>                   | Use the export facility to move content to a remote instance or between stage and production environments: <ul style="list-style-type: none"> <li>■ <a href="#">Exporting an Entire WebCenter Spaces Application</a></li> <li>■ <a href="#">Exporting Group Spaces</a></li> <li>■ <a href="#">Exporting Group Space Templates</a></li> </ul>   | Fusion<br>Middleware<br>Admin |
| <b>Step 11 - Import WebCenter Spaces</b>                   | Use the import facility to restore WebCenter Spaces from a backup or to move content to a remote instance or between stage and production environments: <ul style="list-style-type: none"> <li>■ <a href="#">Importing an Entire WebCenter Spaces Application</a></li> <li>■ <a href="#">Importing Group Spaces</a></li> <li>■ <a href="#">Importing Group Space Templates</a></li> </ul>  | Fusion<br>Middleware<br>Admin |
| <b>Step 12 - View and manage log files</b>                 | Identify and diagnose problems through log files. WebCenter Spaces logs record all types of events, including start up and shutdown information, errors, warnings, and other information: <ul style="list-style-type: none"> <li>■ <a href="#">Viewing and Configuring Log Information</a></li> </ul>  | Fusion<br>Middleware<br>Admin |

**Table 3–1 (Cont.) Roadmap - Administering and Monitoring WebCenter Spaces**

| Step                                 | Documentation  | Role                    |
|--------------------------------------|--|-------------------------|
| <b>Step 13 - Monitor performance</b> | Analyze the performance of WebCenter Spaces and monitor its current status through Fusion Middleware Control Console: <ul style="list-style-type: none"> <li>▪ <a href="#">Viewing Performance Information</a></li> <li>▪ <a href="#">Monitoring WebCenter Spaces</a></li> </ul> | Fusion Middleware Admin |

### 3.4 Application Administration for WebCenter Spaces (Roadmap)

The roadmap in [Table 3–2](#) outlines typical tasks that a WebCenter Spaces administrator might perform while WebCenter Spaces is up and running.

If WebCenter Spaces must be taken offline for maintenance, ensure that a suitable message displays to any users who attempt to access the application while it is offline.

**Table 3–2 Roadmap - Keeping WebCenter Spaces Up and Running**

| Step   | Documentation   | Role                   |
|--|---|------------------------|
| <b>Step 1 - Modify Application Settings</b>  | Modify application-wide settings as required: <ul style="list-style-type: none"> <li>▪ <a href="#">Naming Your WebCenter</a></li> <li>▪ <a href="#">Customizing the Online Help Link</a></li> <li>▪ <a href="#">Choosing the Default Display Language</a></li> <li>▪ <a href="#">Applying Look and Feel using Skins</a></li> <li>▪ <a href="#">Customizing Copyright and Privacy Statements</a></li> <li>▪ ... for more options, see <a href="#">Chapter 18, "Customizing WebCenter Spaces"</a>.</li> </ul> | WebCenter Spaces Admin |
| <b>Step 2 - Manage Personal Spaces</b>       | Manage personal pages and business role pages. Push content to personal spaces: <ul style="list-style-type: none"> <li>▪ <a href="#">Managing Business Role Pages</a></li> <li>▪ <a href="#">Managing Personal Pages</a></li> </ul>   | WebCenter Spaces Admin |
| <b>Step 3 - Manage Group Spaces</b>          | Take any group space temporarily offline and close down any group spaces that is inactive. Manage anyone's group space: <ul style="list-style-type: none"> <li>▪ <a href="#">Viewing Group Space Information</a></li> <li>▪ <a href="#">Changing the Status of a Group Space</a></li> </ul>   | WebCenter Spaces Admin |
| <b>Step 4 - Manage Group Space Templates</b> | Manage group space templates. Review and delete any template: <ul style="list-style-type: none"> <li>▪ <a href="#">Managing Group Space Templates</a></li> </ul>  | WebCenter Spaces Admin |
| <b>Step 5 - Maintain Users and Roles</b>     | Maintain security. Modify user role permissions and assign new roles: <ul style="list-style-type: none"> <li>▪ <a href="#">Modifying Application Role Permissions</a></li> <li>▪ <a href="#">Assigning a User to a Different Role</a></li> </ul>  | WebCenter Spaces Admin |
| <b>Step 6 - Manage the Applications List</b> | Maintain external application links. Add, modify, and delete entries: <ul style="list-style-type: none"> <li>▪ <a href="#">Making an Application Available to WebCenter Users</a></li> <li>▪ <a href="#">Editing Links in the Applications Pane</a></li> <li>▪ <a href="#">Removing Links from the Applications Pane</a></li> </ul>   | WebCenter Spaces Admin |

**Table 3–2 (Cont.) Roadmap - Keeping WebCenter Spaces Up and Running**

| <b>Step</b>                         | <b>Documentation</b>   | <b>Role</b>            |
|-------------------------------------|--|------------------------|
| <b>Step 7- Maintain the Sidebar</b> | Hide Sidebar content when services temporarily unavailable. Expose new services when available: <ul style="list-style-type: none"><li>▪ <a href="#">Hiding and Showing Task Flows in the Sidebar</a></li></ul> | WebCenter Spaces Admin |

---

---

# Getting Custom WebCenter Applications Up and Running

The chapter outlines what Fusion Middleware administrators must do, after installation, to get custom WebCenter applications up and running. A roadmap is provided to help guide you through the process.

The chapter includes the following sections:

- [Installing Oracle WebCenter and Oracle WebCenter Framework Libraries](#)
- [Deploying Custom WebCenter Applications for the First Time \(Roadmap\)](#)

Although WebCenter Spaces is itself a WebCenter application, it does require some special administration tasks that other custom WebCenter applications do not. To see a comprehensive list of these tasks, refer to [Chapter 2, "Getting WebCenter Spaces Up and Running"](#).

## Audience

The content of this chapter is intended for Fusion Middleware administrators responsible for custom WebCenter application administration (users granted the `Admin` role through the Oracle WebLogic Server Administration Console).

## 4.1 Installing Oracle WebCenter and Oracle WebCenter Framework Libraries

Oracle WebCenter installation is described in the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*.

Oracle JDeveloper installation, required for building custom WebCenter applications, is described in *Oracle Fusion Middleware Installation Guide for Oracle JDeveloper*.

Custom WebCenter applications can be deployed to any WebLogic Server instance that is provisioned with the Oracle WebCenter Framework shared library files. For details, see, [Section 7.1.3, "Creating and Provisioning a WebLogic Managed Server Instance"](#).

## 4.2 Deploying Custom WebCenter Applications for the First Time (Roadmap)

The roadmap in [Table 4-1](#) outlines the tasks that a Fusion Middleware administrator must perform to deploy a custom WebCenter application, developed with Oracle WebCenter Framework, and get it up and running.

**Note:** WebCenter Spaces requires additional administration tasks that custom WebCenter applications do not. To see a comprehensive list of these tasks, refer to [Chapter 2, "Getting WebCenter Spaces Up and Running"](#).

**Table 4–1 Roadmap - Getting Custom WebCenter Applications Up and Running for the First Time**

| Step  | Documentation   | Role                          |
|---|---|-------------------------------|
| <b>Step 1 - Verify your Oracle WebCenter installation</b> | <p>Verify your Oracle WebCenter installation and settings. See:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">Installing Oracle WebCenter and Oracle WebCenter Framework Libraries</a></li> <li>▪ <a href="#">Starting Node Manager</a></li> </ul> <p>Installation is described in the <i>Oracle Fusion Middleware Installation Guide for Oracle WebCenter</i>.</p>  | Fusion<br>Middleware<br>Admin |
| <b>Step 2 - Launch Fusion Middleware Control</b>          | <p>Launch the Fusion Middleware Control Console, a Web-based management tool for WebCenter applications. See:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">Displaying Fusion Middleware Control Console</a></li> <li>▪ <a href="#">Navigating to the Home Page for Custom WebCenter Applications</a></li> </ul> <p>Learn about the command-line administration tool WLST. See "Oracle WebLogic Scripting Tool (WLST)".</p>  | Fusion<br>Middleware<br>Admin |
| <b>Step 3 - Deploy the custom WebCenter application</b>   | <p>Create a suitable container in which to deploy the custom WebCenter application archive:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">Creating and Provisioning a WebLogic Managed Server Instance</a></li> <li>▪ <a href="#">Creating and Registering the Metadata Service (MDS) Repository</a></li> <li>▪ <a href="#">Deploying a WebCenter Application to a WebLogic Managed Server Instance</a></li> </ul> <p>See also, "Deploying WebCenter Applications".</p>  | Fusion<br>Middleware<br>Admin |
| <b>Step 4 - Connect back-end services</b>                 | <p>Configure back-end services for the custom WebCenter application through Fusion Middleware Control.</p> <ul style="list-style-type: none"> <li>▪ <b>Content Repositories</b> <ul style="list-style-type: none"> <li>▪ <a href="#">Managing Content Repositories</a></li> </ul> </li> <li>▪ <b>Mail Servers</b> <ul style="list-style-type: none"> <li>▪ <a href="#">Setting Up Connections for the Mail Service</a></li> </ul> </li> <li>▪ <b>BPEL Servers</b> <ul style="list-style-type: none"> <li>▪ <a href="#">Setting Up Worklist Connections</a></li> </ul> </li> <li>▪ <b>Collaboration Services</b> <ul style="list-style-type: none"> <li>▪ <a href="#">Setting Up Connections for the Discussions and Announcements Services</a></li> <li>▪ <a href="#">Setting Up Connections for the Instant Messaging and Presence Service</a></li> </ul> </li> <li>▪ <b>Secure Enterprise Search</b> <ul style="list-style-type: none"> <li>▪ <a href="#">Setting Up Connections for the Search Service</a></li> </ul> </li> <li>▪ <b>Wiki and Blog Services</b> <ul style="list-style-type: none"> <li>▪ <a href="#">Setting Up the Server for Wiki and Blog Services</a></li> </ul> </li> <li>▪ <b>External Applications</b> <ul style="list-style-type: none"> <li>▪ <a href="#">Managing External Applications</a></li> </ul> </li> </ul> | Fusion<br>Middleware<br>Admin |



**Table 4–1 (Cont.) Roadmap - Getting Custom WebCenter Applications Up and Running for the First Time**

| Step   | Documentation   | Role                          |
|--|---|-------------------------------|
| <ul style="list-style-type: none"> <li>■ Portlet Producers</li> <li>■ Group Space Events, Links, Lists, Notes, and Tags</li> </ul> | <ul style="list-style-type: none"> <li>■ <a href="#">Registering WSRP Producers</a></li> <li>■ <a href="#">Registering Oracle PDK-Java Producers</a></li> <li>■ <a href="#">Setting Up the WebCenter Repository</a></li> <li>■ <a href="#">Setting Up the MDS Repository</a></li> </ul> |                               |
| <b>Step 5 - Connect to an identity store</b>   | <p>Ensure that your identity store is installed, configured, and contains all the required user data. See:</p> <ul style="list-style-type: none"> <li>■ <a href="#">Configuring the Identity Store</a></li> </ul> <p>See also <i>Oracle Fusion Middleware Security Guide</i>.</p>       | Fusion<br>Middleware<br>Admin |
| <b>Step 6 - Restart the managed server</b>   | <p>Restart the managed server on which the application is deployed. See:</p> <ul style="list-style-type: none"> <li>■ <a href="#">Starting and Stopping Managed Servers for WebCenter Application Deployments</a></li> </ul>  | Fusion<br>Middleware<br>Admin |
| <b>Step 7 - Verify custom WebCenter application configuration</b>  | <p>Login to the application to verify the configuration: identity store, services, applications, and so on.</p>   | Fusion<br>Middleware<br>Admin |



---



---

## Maintaining Custom WebCenter Applications

The chapter outlines what Fusion Middleware administrators might do to keep custom WebCenter applications up and running. The following roadmap will help guide you through the process:

- [System Administration for Custom WebCenter Applications \(Roadmap\)](#)

Although WebCenter Spaces is itself a WebCenter application, it does require some special maintenance tasks that custom WebCenter applications do not. To see a comprehensive list of these tasks, refer to [Chapter 3, "Maintaining WebCenter Spaces"](#).

### Audience

The content of this chapter is intended for Fusion Middleware administrators responsible for custom WebCenter application administration (users granted the `Admin` role through the Oracle WebLogic Server Administration Console).

## 5.1 System Administration for Custom WebCenter Applications (Roadmap)

The roadmap in [Table 5–1](#) outlines typical tasks that a Fusion Middleware administrator might perform to keep a custom WebCenter application up and running.

If the custom WebCenter application must temporarily shut down for maintenance, ensure that a suitable message displays to any users who attempt to access the application while it is offline.

**Table 5–1 Roadmap - Maintaining Custom WebCenter Applications**

| Step  | Documentation  | Role                    |
|---|--|-------------------------|
| <b>Step 1 - Stop and start the managed server</b>               | Restart the managed server on which the custom WebCenter application is deployed to effect configuration changes or for routine maintenance: <ul style="list-style-type: none"> <li>▪ <a href="#">Starting and Stopping Managed Servers for WebCenter Application Deployments</a></li> </ul> | Fusion Middleware Admin |
| <b>Step 2 - Stop and start the custom WebCenter application</b> | Shut down the application for maintenance purposes and then restart the application: <ul style="list-style-type: none"> <li>▪ <a href="#">Starting and Stopping Custom WebCenter Applications</a></li> </ul>   | Fusion Middleware Admin |
| <b>Step 3 Maintain back-end services</b>                        | Add, modify, and delete connections through the Fusion Middleware Control Console: <ul style="list-style-type: none"> <li>▪ <a href="#">Managing Content Repositories</a></li> </ul>   | Fusion Middleware Admin |
| ▪ <b>Content Repositories</b>                                   |  |                         |

**Table 5–1 (Cont.) Roadmap - Maintaining Custom WebCenter Applications**

| Step   | Documentation   | Role                    |
|--|---|-------------------------|
| <ul style="list-style-type: none"> <li>▪ Mail Servers</li> <li>▪ BPEL Servers</li> <li>▪ Collaboration Services</li> <li>▪ Secure Enterprise Search</li> <li>▪ Wiki and Blog Services</li> </ul> | <ul style="list-style-type: none"> <li>▪ <a href="#">Setting Up Connections for the Mail Service</a></li> <li>▪ <a href="#">Setting Up Worklist Connections</a></li> <li>▪ <a href="#">Setting Up Connections for the Discussions and Announcements Services</a></li> <li>▪ <a href="#">Setting Up Connections for the Instant Messaging and Presence Service</a></li> <li>▪ <a href="#">Setting Up Connections for the Search Service</a></li> <li>▪ <a href="#">Setting Up the Server for Wiki and Blog Services</a></li> </ul>   |                         |
| <b>Step 4 - Maintain external applications and portlet producers</b>   | Add, modify, and delete connections through Oracle Enterprise Manager Fusion Middleware Control Console. See:   | Fusion Middleware Admin |
| <ul style="list-style-type: none"> <li>▪ External Applications</li> <li>▪ Portlet Producers</li> </ul>   | <ul style="list-style-type: none"> <li>▪ <a href="#">Managing External Applications</a></li> <li>▪ <a href="#">Registering WSRP Producers</a></li> <li>▪ <a href="#">Registering Oracle PDK-Java Producers</a></li> </ul>   |                         |
| <b>Step 5 - Reconfigure your identity store</b>  | <ul style="list-style-type: none"> <li>▪ <a href="#">Configuring the Identity Store</a></li> </ul> See also, <i>Oracle Fusion Middleware Security Guide</i> .   | Fusion Middleware Admin |
| <b>Step 6 - Reconfigure the MDS repository</b>   | <ul style="list-style-type: none"> <li>▪ <a href="#">Setting Up the MDS Repository</a></li> </ul>   | Fusion Middleware Admin |
| <b>Step 7 - Reconfigure WebCenter repository</b>   | <ul style="list-style-type: none"> <li>▪ <a href="#">Setting Up the WebCenter Repository</a></li> </ul>   |                         |
| <b>Step 8 - Export custom WebCenter application data</b>   | Migrate data to a remote instance or between stage and production environments: <ul style="list-style-type: none"> <li>▪ <a href="#">Exporting WebCenter Web 2.0 Services Metadata and Data (Custom WebCenter Applications)</a></li> <li>▪ <a href="#">Exporting Portlet Client Metadata (Custom WebCenter Applications)</a></li> <li>▪ <a href="#">Migrating Security for Custom WebCenter Applications</a></li> <li>▪ <a href="#">Migrating Data (Custom WebCenter Applications)</a></li> </ul> See also, "Managing Export, Import, Backup, and Recovery of WebCenter". | Fusion Middleware Admin |
| <b>Step 9 - Import custom WebCenter application data</b>   | Use the import facility to move content to a remote instance or between stage and production environments: <ul style="list-style-type: none"> <li>▪ <a href="#">Importing WebCenter Web 2.0 Services Metadata and Data (Custom WebCenter Applications)</a></li> <li>▪ <a href="#">Importing Portlet Client Metadata (Custom WebCenter Applications)</a></li> <li>▪ <a href="#">Migrating Security for Custom WebCenter Applications</a></li> <li>▪ <a href="#">Migrating Data (Custom WebCenter Applications)</a></li> </ul>  | Fusion Middleware Admin |

**Table 5–1 (Cont.) Roadmap - Maintaining Custom WebCenter Applications**

| <b>Step</b>                                  | <b>Documentation</b>  | <b>Role</b>                   |
|--|---|-------------------------------|
| <b>Step 10 - View and manage log files</b>   | Identify and diagnose problems through log files. Custom WebCenter application logs record all types of events, including start up and shutdown information, errors, warnings, and other information: <ul style="list-style-type: none"> <li>▪ <a href="#">Viewing and Configuring Log Information</a></li> </ul> | Fusion<br>Middleware<br>Admin |
| <b>Step 11 - Monitor performance</b>         | Analyze the performance of the custom WebCenter application and monitor its current status through Fusion Middleware Control Console: <ul style="list-style-type: none"> <li>▪ <a href="#">Viewing Performance Information</a></li> <li>▪ <a href="#">Monitoring Custom WebCenter Applications</a></li> </ul>     | Fusion<br>Middleware<br>Admin |
| <b>Step 12 - Tune application properties</b> | <ul style="list-style-type: none"> <li>▪ <a href="#">Tuning Environment Configuration</a></li> <li>▪ <a href="#">Tuning WebCenter Application Configuration</a></li> <li>▪ <a href="#">Tuning Back-End Component Configuration</a></li> </ul>   | Fusion<br>Middleware<br>Admin |



# Part III

---

## Basic Systems Administration for Oracle WebCenter

This part of the Administrator's Guide presents system administration tasks for Oracle WebCenter and WebCenter applications, such as, WebCenter Spaces and any custom WebCenter applications that you deploy.

Part III contains the following chapters:

- [Chapter 6, "Starting Enterprise Manager Fusion Middleware Control"](#)
- [Chapter 7, "Deploying WebCenter Applications"](#)
- [Chapter 8, "Starting and Stopping WebCenter Applications"](#)
- [Chapter 9, "Setting Application Properties"](#)
- [Chapter 10, "Managing Content Repositories"](#)
- [Chapter 11, "Managing Services"](#)
- [Chapter 12, "Managing Portlet Producers"](#)
- [Chapter 13, "Managing External Applications"](#)





---

# Starting Enterprise Manager Fusion Middleware Control

This chapter describes how to access Oracle Enterprise Manager Fusion Middleware Control Console, and display WebCenter-related pages from where you can perform all necessary configuration, monitoring, and management tasks.

This chapter includes the following sections:

- [Displaying Fusion Middleware Control Console](#)
- [Navigating to the Home Page for WebCenter Spaces](#)
- [Navigating to the Home Page for Custom WebCenter Applications](#)
- [Navigating to Dependent Components](#)

## Audience

The content of this chapter is intended for Fusion Middleware administrators (users granted the `Admin`, `Operator`, or `Monitor` role through the Oracle WebLogic Server Administration Console). See also, [Section 1.8, "Understanding Administrative Operations, Roles, and Tools"](#).

## 6.1 Displaying Fusion Middleware Control Console

Fusion Middleware administrators can login to Fusion Middleware Control Console and access Oracle WebCenter pages. Your role determines what you can see and do after logging in. To find out more, see [Table 1–5, "WebCenter Operations and Oracle WebLogic Server Roles"](#).

To access the Fusion Middleware Control Console:

1. Start Fusion Middleware Control.

Fusion Middleware Control is configured for a domain, and it is automatically started when you start the Oracle WebLogic Server Administration Server. See "Starting and Stopping Fusion Middleware Control" in *Oracle Fusion Middleware Administrator's Guide*.

2. Navigate to the following URL: `http://host_name.domain_name:port_number/em`

For example: `http://myhost.mycompany.com:7001/em`

You can find the exact URL, including the administration port number, in `config.xml`:

- On Windows: `DOMAIN_HOME\config\config.xml`

- On UNIX: DOMAIN\_HOME/config/config.xml

See also, "Managing Ports" in *Oracle Fusion Middleware Administrator's Guide*.

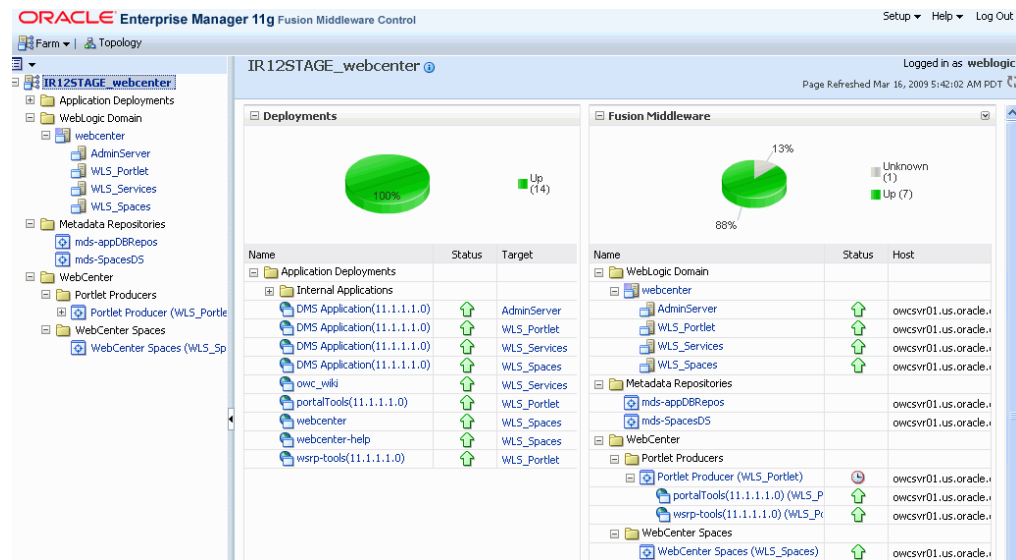
3. Enter a valid administrator **User Name** and **Password** details for the farm.

The default user name for the administrator user is `weblogic`. This is the account you can use to log in to Fusion Middleware Control for the first time.

4. Click **Login**.

The first page you see is the Farm home page. You can also view this page at any time by selecting the name of the farm in the navigation pane ([Figure 6-1](#)).

**Figure 6-1 Farm Home Page**



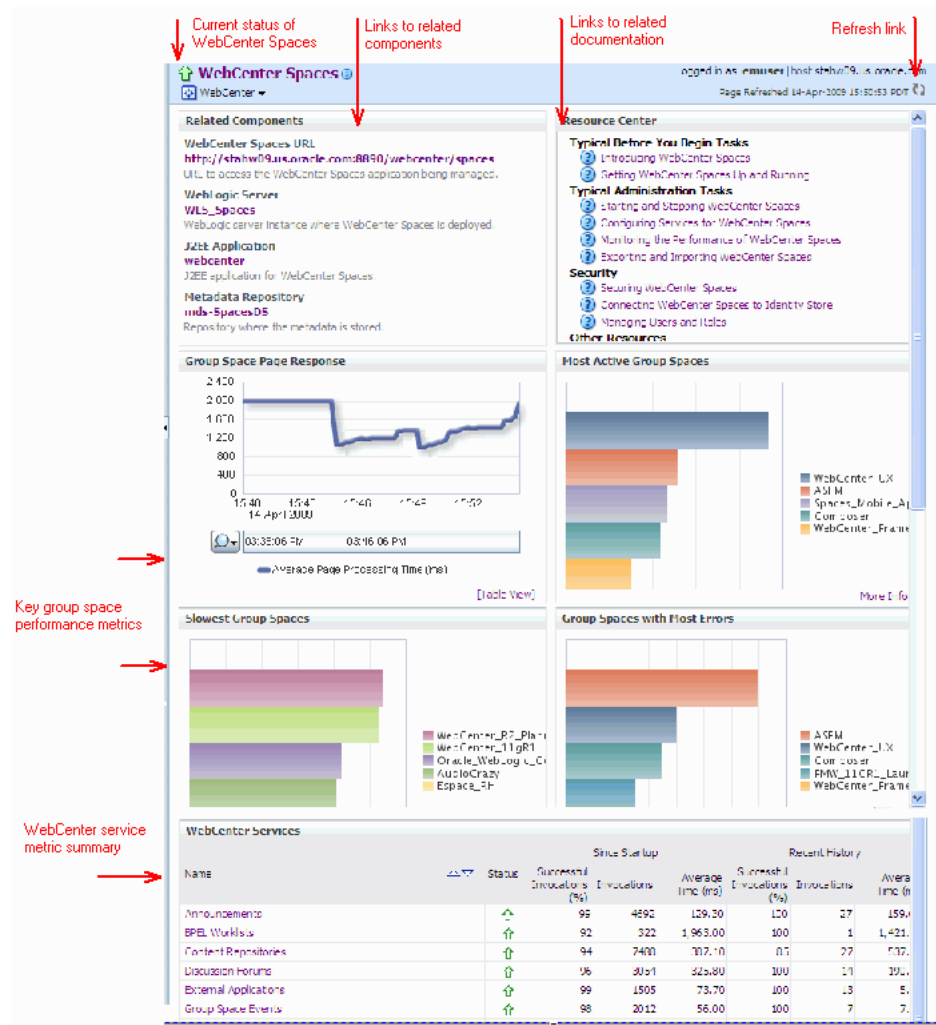
From the navigation pane, you can drill down to view and manage all components in your farm, including WebCenter Spaces and any custom WebCenter applications that you may have deployed. For detailed instructions, see

- [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#).
- [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#).

## 6.2 Navigating to the Home Page for WebCenter Spaces

The WebCenter Spaces home page is your starting place for managing WebCenter Spaces. The page displays status, performance and availability of all the components and services that make up WebCenter Spaces.

Figure 6–2 WebCenter Spaces Home Page

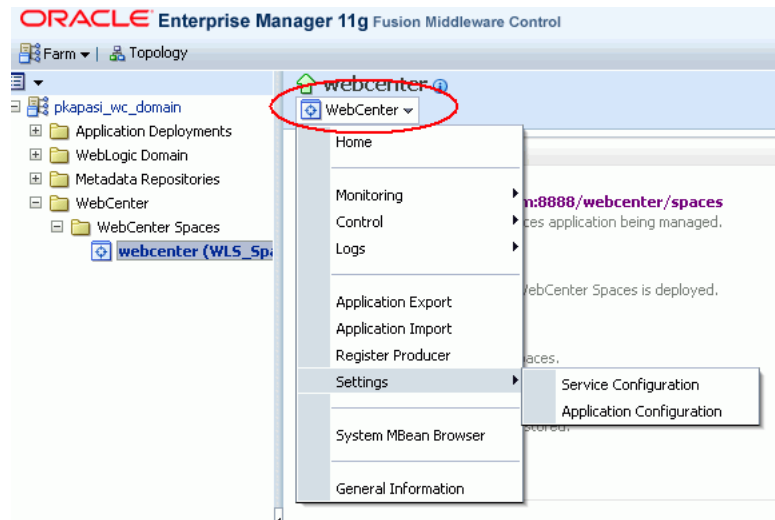


From here you can:

- Check the status of WebCenter Spaces.
- View key group space performance data and track overall response time. Quickly see which group spaces are used the most, the slowest performers, and determine which group spaces are recording the most errors.
- Navigate to key WebCenter Spaces components, including the application itself, WebLogic Server installation, MDS repository, and the deployed J2EE application.
- View status and key performance metrics for WebCenter services used in the application.
- Drill down to detailed performance information for individual group spaces, services, external applications, portlets, and producers.

The WebCenter Spaces home page also displays a **WebCenter menu** (Figure 6–3).

**Figure 6–3 WebCenter Menu for WebCenter Spaces**



From the WebCenter menu, you can:

- Start and stop WebCenter Spaces
- Configure application settings
- Manage back-end services
- Manage external applications
- Manage portlet producers
- Monitor detailed performance metrics for all components
- Select and chart live metrics
- Analyze diagnostic information and configure logs
- Export and import WebCenter Spaces

To navigate to the main home page for WebCenter Spaces:

1. Login to Fusion Middleware Control.  
See [Section 6.1, "Displaying Fusion Middleware Control Console"](#).
2. In the Navigator ([Figure 6–4](#)), expand WebCenter.

**Figure 6–4 Navigating to the WebCenter Spaces Home Page**

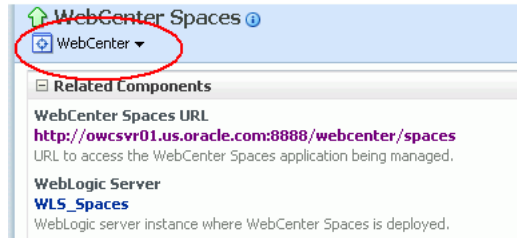


3. Expand **WebCenter Spaces**.

4. Select **WebCenter Spaces** to navigate to the home page for your WebCenter Spaces installation.

Notice how the Navigator menu changes to *WebCenter* (Figure 6–5).

**Figure 6–5** *Displaying the WebCenter Spaces Home Page and Menu*

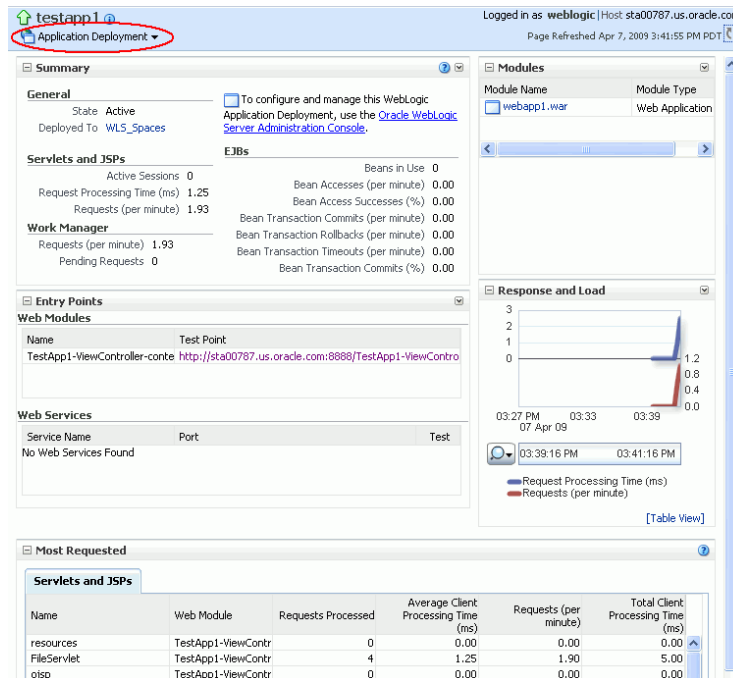


### 6.3 Navigating to the Home Page for Custom WebCenter Applications

The J2EE Application Deployment home page (Figure 6–6) is your starting place for managing custom WebCenter application deployments developed with Oracle WebCenter Framework. The page displays status, performance and availability of all the components and services that make up the custom WebCenter application.

**Note:** WebCenter Spaces has a different home page, see [Navigating to the Home Page for WebCenter Spaces](#).

**Figure 6–6** *Custom WebCenter Application Home Page*



From here you can:

- Check custom WebCenter application status.
- Navigate to the Oracle WebLogic Server Administration Console.

- Access various Application Deployment menu options:
  - Start, restart, and shutdown the application
  - View and configure log files.
  - Undeploy and redeploy the application.
  - Configure security policies and roles.
  - Configure ADF and MDS options.
- View a performance summary, entry points to the application, Web Services and modules associated with the application, and the response and load data which shows the requests per second and the request processing time.
- Navigate to key components of the custom WebCenter application.
- Drill down to detailed performance information for individual modules and services.

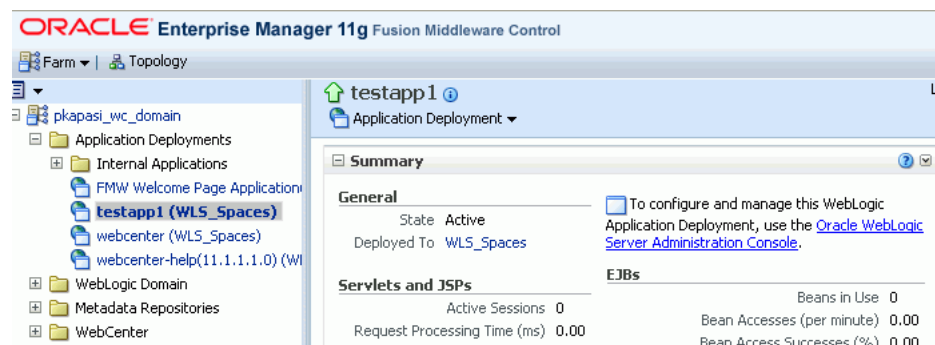
For custom WebCenter applications, the Application Deployment menu displays an additional menu option—*WebCenter*. From the WebCenter menu, you can perform WebCenter-specific tasks such as:

- Manage external applications (see [Chapter 13, "Managing External Applications"](#)).
- Manage back-end services (see [Chapter 11, "Managing Services"](#)).
- Manage portlet producers (see [Chapter 12, "Managing Portlet Producers"](#)).
- Monitor detailed performance metrics for WebCenter services (see [Chapter 15, "Monitoring Oracle WebCenter Performance"](#)).

To navigate to the main home page for your custom WebCenter application:

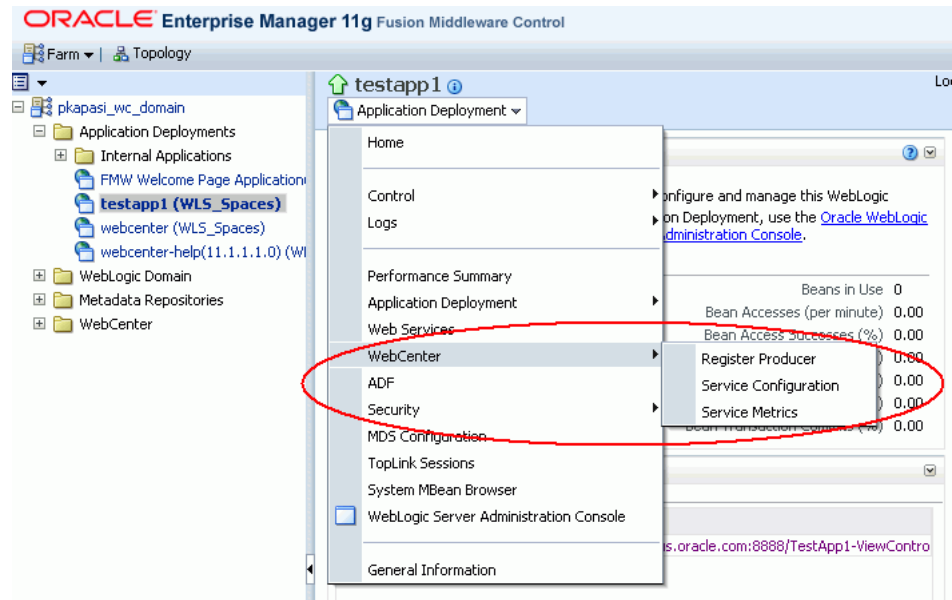
1. Login to Fusion Middleware Control.  
See [Section 6.1, "Displaying Fusion Middleware Control Console"](#).
2. In the Navigator ([Figure 6–7](#)), expand **Application Deployments**.

**Figure 6–7 Navigating to a Custom WebCenter Application Home Page**



3. Select the name of your custom WebCenter application to display the application's home page.  
Notice WebCenter menu options display on the **Application Deployment** menu ([Figure 6–8](#)).

**Figure 6–8** *Displaying the Custom WebCenter Application Home Page and Menu*



## 6.4 Navigating to Dependent Components

From WebCenter application pages it is easy to navigate to pages belonging to related components, such as, WebLogic Server domains, servers, Java components, MDS repository, and so on.

- WebCenter Spaces** - From the home page, click links in "Related Components" to navigate to the WebCenter Spaces application itself, as well as WebLogic Server installation pages, MDS repository pages, and J2EE application pages in Fusion Middleware Control. See also, [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#).

From the J2EE application page you can also access ADF and security information.

- Custom WebCenter applications** - The Application Deployment menu on the J2EE application home page offers direct navigation to the Oracle WebLogic Server Administration Console, as well as pages relating to ADF, MDS repository, and security. See also, [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#).





---

---

## Deploying WebCenter Applications

This chapter provides instructions for deploying, undeploying, and redeploying custom WebCenter applications from an Enterprise Archive, or .EAR file, created with Oracle JDeveloper (for information on how to create an .EAR file, see "How to Create Deployment Profiles in Oracle JDeveloper" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*). It does not contain instructions for deploying or installing Oracle WebCenter Spaces. For information about installing Oracle WebCenter Spaces and other WebCenter components, see "Installing Oracle WebCenter" in the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*. For information about deploying WSRP and PDK-Java portlet producer applications, see [Section 12.8, "Deploying Portlet Producer Applications."](#)

This chapter includes the following sections:

- [Deploying Custom WebCenter Applications](#)
- [Undeploying Custom WebCenter Applications](#)
- [Redeploying Custom WebCenter Applications](#)

### Audience

The content of this chapter is intended for Fusion Middleware administrators (users granted the `Admin` role through the Oracle WebLogic Server Administration Console). See also, [Section 1.8, "Understanding Administrative Operations, Roles, and Tools."](#)

## 7.1 Deploying Custom WebCenter Applications

This section describes the steps required to deploy a custom WebCenter application, which has been created in JDeveloper, to a production domain. The deployment steps in this section assume that you have created an .EAR file, know its location, and that the domain to which you want to deploy already exists.

For information on how to create a new WebLogic Server domain, see "Creating a New Domain" in the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*. For more information about deploying WebCenter applications, see the *Oracle Fusion Middleware Deploying Applications to Oracle WebLogic Server*.

This section includes the following topics:

- [Understanding Custom WebCenter Application Deployment](#)
- [Creating the .EAR File](#)
- [Creating and Registering the Metadata Service \(MDS\) Repository](#)
- [Creating and Provisioning a WebLogic Managed Server Instance](#)

- [Deploying a WebCenter Application to a WebLogic Managed Server Instance](#)
- [Transporting Customizations Between Environments](#)
- [Configuring WebCenter Applications to Run in a Distributed Environment](#)

## 7.1.1 Understanding Custom WebCenter Application Deployment

You can deploy custom WebCenter applications to any WebLogic managed server instance that is provisioned with the Oracle WebCenter libraries.

---

---

**Note:** Oracle does not recommend deploying custom WebCenter applications to any of the three pre-configured managed servers created during the installation, or to the Administration Server. For WebCenter applications created in JDeveloper, follow the process described in [Section 7.1.4, "Creating and Registering the Metadata Service \(MDS\) Repository"](#) and [Section 7.1.3, "Creating and Provisioning a WebLogic Managed Server Instance"](#) to create and provision a new WLS managed server prior to deploying.

---

---

The process consists of:

- [Creating the .EAR File](#)
- [Creating and Provisioning a WebLogic Managed Server Instance](#)
- [Creating and Registering the Metadata Service \(MDS\) Repository](#)
- [Deploying a WebCenter Application to a WebLogic Managed Server Instance](#)

## 7.1.2 Creating the .EAR File

Before you deploy an application, you must first create an .EAR file for it. For information on how to create an .EAR file for an application, see "How to Create Deployment Profiles in Oracle JDeveloper" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

The .EAR file packages multiple information artifacts, which include:

- The application itself: the physical pieces of the application such as .jsp, .jar, and .class files.
- Application Configuration -- which contains the URL endpoints and properties of connections to services and producers that are configured for this application.
- Application Metadata -- which is an export of the application metadata created during the design time of the application.
- Portlet Customizations -- which contain customization settings and data for portlets. This information is maintained within the producer, but is exported when an application with registered producers is packaged. This customization data is packaged with the rest of the metadata of a custom WebCenter application.

## 7.1.3 Creating and Provisioning a WebLogic Managed Server Instance

Before deploying a custom WebCenter application, you must also create a new WebLogic managed server instance and provision it with a required set of shared libraries. You can create a WebLogic managed server instance using the WLS Administration Console, or using Fusion Middleware Control. You can also create a WebLogic managed server instance and provision it using WLST, by means of a Jython

script. A sample Jython script that you can modify to suit the needs of your local environment is available for download from the Oracle Technology Network (OTN) at [http://www.oracle.com/technology/products/webcenter/release11\\_demos.html](http://www.oracle.com/technology/products/webcenter/release11_demos.html) under Administration Samples. These three options are described in the following sections:

- [Creating a WebLogic Managed Server Using the WLS Administration Console](#)
- [Creating a WebLogic Managed Server Using Fusion Middleware Control](#)
- [Creating and Provisioning a WebLogic Managed Server Using a Jython Script](#)

### 7.1.3.1 Creating a WebLogic Managed Server Using the WLS Administration Console

You can create a WebLogic managed server on an existing domain using the WLS Administration Console to create the server instance and provision the shared libraries required to run a custom WebCenter application.

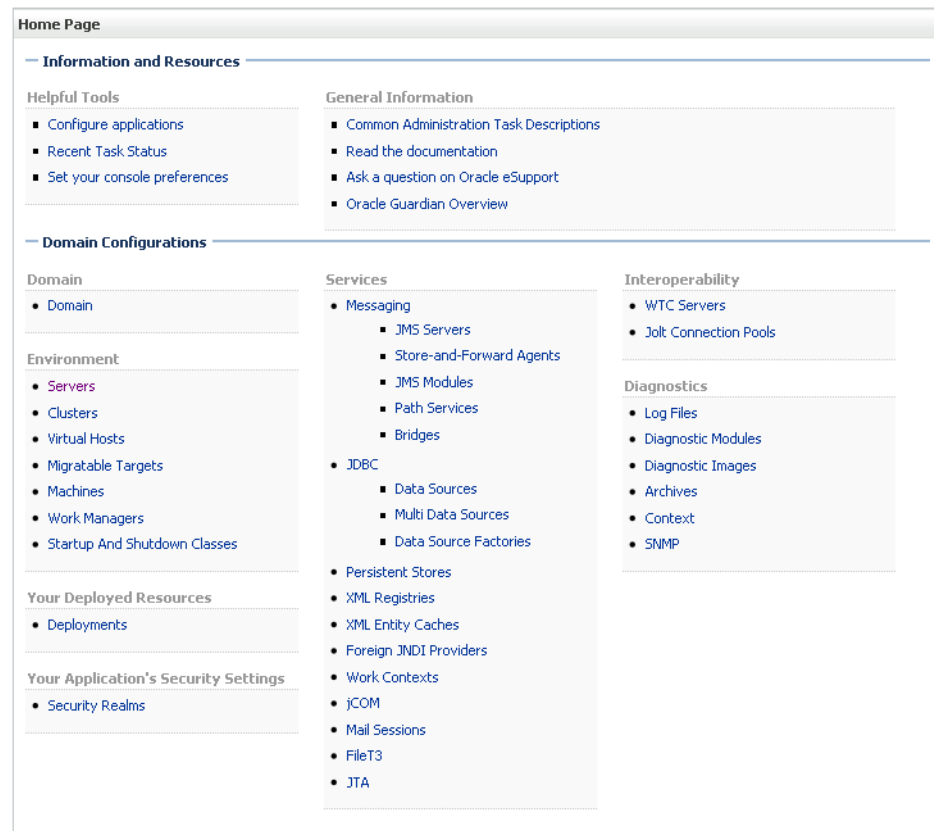
To create a WebLogic Managed Server using the WLS Administration Console:

1. Log in to the WLS Administration Console.

For information on logging into the WLS Administration Console, see [Section 1.12.2, "Oracle WebLogic Server Administration Console."](#)

2. Navigate to the WLS Administration Console's Home page (see [Figure 7-1](#)).

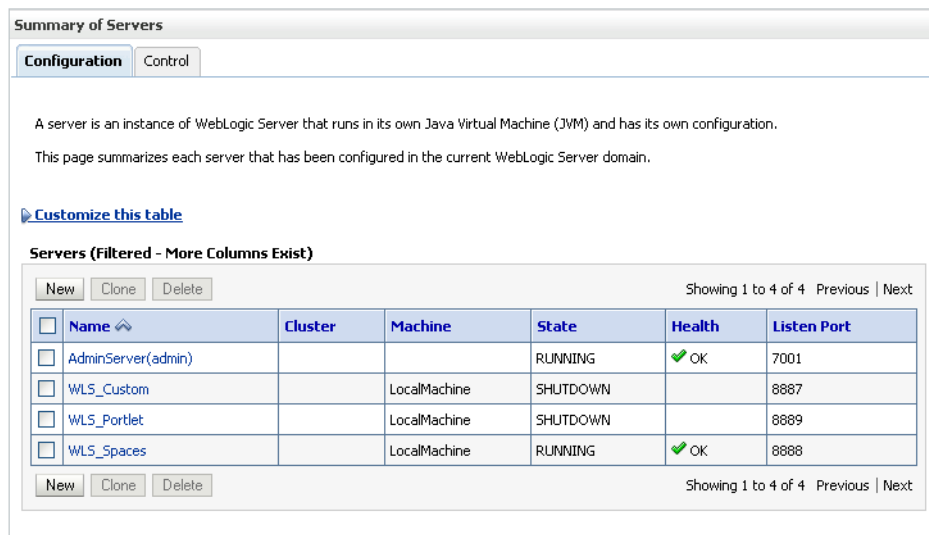
**Figure 7-1 WLS Administration Console Home Page**



3. From the WLS Administration Console's Home page under **Domain Configurations**, click **Servers**.

The Summary of Servers pane displays (see [Figure 7-2](#)).

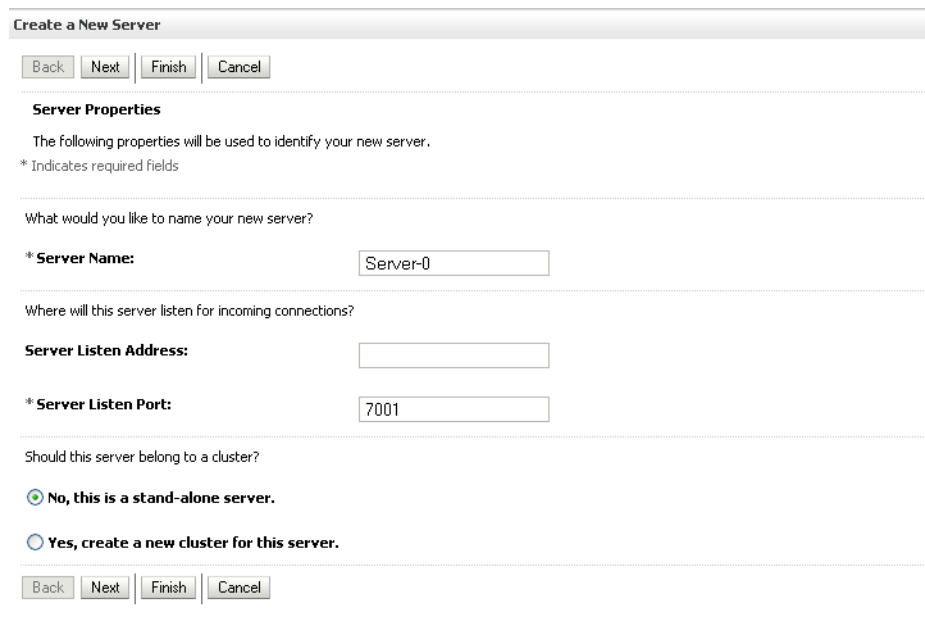
**Figure 7-2 Summary of Servers Pane**



- On the Summary of Servers pane, click **New** to create a new WebLogic managed server instance.

The Create a New Server pane displays (see [Figure 7-3](#)).

**Figure 7-3 Create a New Server pane**



- Enter a **Server Name** for the new managed server, and the **Port Number** to be assigned to it. Leave the default settings for the rest of the fields.

---



---

**Note:** Do not set the port number to 7001 as this port number is used by the domain administration server. Also do not leave the port number blank as it defaults to 7001.

---



---

6. Click **Finish**, then **Save** to generate the new managed server.
7. On the Domain Structure pane, click **Deployment**.

In this step, we will provision the new managed server with the shared libraries required to run a custom WebCenter application. Several shared libraries will already have been deployed, but you also need to make sure that the required libraries are targeted to the newly created managed server.

---



---

**Note:** If you have set up a cluster with several WebLogic managed servers in your WebLogic domain, target all libraries to the cluster instead. All managed servers in the cluster will inherit from the cluster automatically.

---



---

The shared libraries required are different to host a custom WebCenter application that will consume portlets than for a portlet producer application. If you want the server to run both consumer and producer applications you will need to deploy both sets of shared libraries.

For a custom WebCenter application that will consume portlets *only*, you must deploy the following libraries to the new managed server or cluster:

- `adf.oracle.domain(1.0,11.1.1.0.0)`
- `adf.oracle.domain.webapp(1.0,11.1.1.1.0)`
- `jsf(1.2,1.2.9.0)`
- `jstl(1.2,1.2.0.1)`
- `ohw-rcf(5,5.0)`
- `ohw-uix(5,5.0)`
- `UIX(11,11.1.1.1.0)`
- `oracle.adf.dconfigbeans(1.0,11.1.1.0.0)`
- `oracle.adf.management(1.0,11.1.1.1.0)`
- `oracle.dconfig-infra`
- `oracle.jrf.system.filter`
- `oracle.jsp.next(11.1.1,11.1.1)`
- `oracle.sdp.client(11.1.1,11.1.1)`
- `oracle.soa.workflow.wc(11.1.1,11.1.1)`
- `oracle.webcenter.framework(11.1.1,11.1.1)`
- `oracle.webcenter.framework.view(11.1.1,11.1.1)`
- `oracle.webcenter.jive.dependency(11.1.1,11.1.1)`
- `oracle.webcenter.skin(11.1.1,11.1.1)`
- `oracle.wsm.seedpolicies(11.1.1,11.1.1)`

- `oracle.portlet-producer.jpdk(11.1.1,11.1.1)`
- `oracle.portlet-producer.wsrp(11.1.1,11.1.1)`

---

**Note:** If the two shared libraries `oracle.portlet-producer.jpdk` and `oracle.portlet-producer.wsrp` are not available from the WLS console, you need to install them by running the configuration wizard again and selecting the **Portlet** checkbox. If these two libraries are not provisioned to the new managed server, portlet-specific functions will not work in a custom WebCenter application.

---

For a portlet producer application, the following libraries must be deployed to the new managed server or cluster:

- `adf.oracle.domain(1.0,11.1.1.0.0)`
  - `adf.oracle.domain.webapp(1.0,11.1.1.1.0)`
  - `jsf(1.2,1.2.9.1)`
  - `jstl(1.2,1.2.0.1)`
  - `ohw-rcf(5,5.0)`
  - `ohw-uix(5,5.0)`
  - `UIX(11,11.1.1.1.0)`
  - `oracle.adf.dconfigbeans(1.0,11.1.1.0.0)`
  - `oracle.dconfig-infra`
  - `oracle.jrf.system.filter`
  - `oracle.jsp.next(11.1.1,11.1.1)`
  - `oracle.webcenter.skin(11.1.1,11.1.1)`
  - `oracle.wsm.seedpolicies(11.1.1,11.1.1)`
  - `oracle.portlet-producer.jpdk(11.1.1,11.1.1)`
  - `oracle.portlet-producer.wsrp(11.1.1,11.1.1)`
8. In addition, for both WebCenter and portlet producer applications, you also need to deploy the following applications:
- DMS application
  - `wsm-pm`

For each shared library or application to add:

- Click the library or application link.
  - Open the Target tab for the library or application.
  - Supply the target to the newly created managed server.
9. Select the checkbox of the new managed server and click **Save**.
10. On the Domain Structure pane, expand Environment and click **Startup and Shutdown classes**. The following classes should show as available:
- Audit Loader Startup Class

- DMS-Startup
- DMS-Shutdown
- JMX Framework Startup Class
- JOC-Shutdown
- JOC-Startup
- JPS-Startup Class
- JRF Startup Class
- ODL-Startup
- OWSM Startup Class

---

**Note:** The actual startup and shutdown classes may differ depending on your setup and installation options. All startup and shutdown classes that appear should be targeted to the newly created managed server instance.

---

11. For each class in the list above:

- Click the class name.
- On the Target tab, check the newly created managed server.
- Click **Save**.

12. When all the shared libraries and application assignments are complete, do one of the following:

- Start the new managed server using Fusion Middleware Control as described in [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."](#)
- Start the new managed server by opening a terminal window and invoking the following command from your domain's /bin directory (under wls\_home/user\_projects unless the default location has been changed):

```
nohup ./startManagedWebLogic.sh custom_server_id http://server_ip_
addr:server_port_num
-Dweblogic.management.username=user_name
-Dweblogic.management.password=password customServer.out &
```

Where:

- custom\_server\_id is the name of the new managed server you created (for example, CustomAppServer3).
- server\_ip\_addr is the IP address of the administration server.
- server\_port\_num is the port number of the administration server.
- user\_name is the user name to access the server (for example, weblogic).
- password is the password to access the server (for example, weblogic).

Once the managed server is started, you can continue to deploy your WebCenter application as described in [Section 7.1.5, "Deploying a WebCenter Application to a WebLogic Managed Server Instance,"](#) or portlet producer

application as described in [Section 12.8, "Deploying Portlet Producer Applications."](#)

### 7.1.3.2 Creating a WebLogic Managed Server Using Fusion Middleware Control

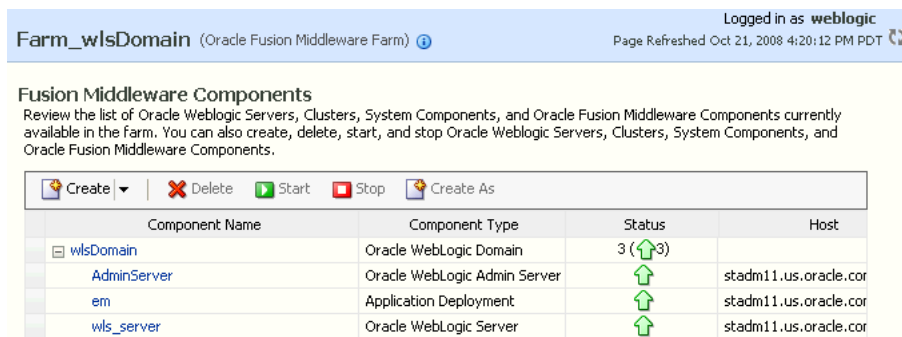
Use Fusion Middleware Control to create a new WebLogic managed server instance for custom WebCenter application deployment.

**Note:** Although you can create a WebLogic managed server using Fusion Middleware Control, you must use the WebLogic Administration Console to provision it as described in [Section 7.1.3.1, "Creating a WebLogic Managed Server Using the WLS Administration Console,"](#) or modify the Jython script described in [Section 7.1.3.3, "Creating and Provisioning a WebLogic Managed Server Using a Jython Script"](#) to provision the shared libraries required to run a custom WebCenter application.

To create a new WebLogic managed server using Fusion Middleware Control:

1. Log in to Fusion Middleware Control.  
See [Section 6.1, "Displaying Fusion Middleware Control Console."](#)
2. From the Farm menu, choose **Create/Delete Components**.  
The Fusion Middleware Components page opens ([Figure 7–4](#)).

**Figure 7–4 Fusion Middleware Components Page**



3. From the Create menu, select **WebLogic Server**.
4. Enter a unique name for the WebLogic server (for example, myWebCenterWLS, as shown in [Figure 7–5](#)).



**Figure 7-5 Create WebLogic Server Page**

5. Under Weblogic Machine, create or select the application server instance where this WebLogic managed server instance should be created.
6. Click **Create**.
7. When the Confirmation page displays, click **Close**.
8. In the Fusion Middleware Components page, select the new WebLogic managed server instance, and click **Start**.
9. Continue by provisioning the shared libraries as described in [Section 7.1.3.1, "Creating a WebLogic Managed Server Using the WLS Administration Console"](#) omitting the steps (steps 4 to 7) for creating the managed server, or using a modified version of the Jython script described in [Section 7.1.3.3, "Creating and Provisioning a WebLogic Managed Server Using a Jython Script."](#)

### 7.1.3.3 Creating and Provisioning a WebLogic Managed Server Using a Jython Script

You can use a Jython script to automate the process of creating a new managed server instance. An example script that you can modify for your local environment is available for download from the Oracle WebCenter Suite 11g Demonstrations and Samples page on OTN at:

[http://www.oracle.com/technology/products/webcenter/release11\\_demos.html](http://www.oracle.com/technology/products/webcenter/release11_demos.html)

The example script creates a new WebLogic managed server instance, deploys the shared libraries required to run a WebCenter application, and checks that the new managed server is ready for deployment.

To create and provision WebLogic Managed Server using a Jython script:

1. Download the example script from OTN.
2. Copy the following two files into your `MWHOME/as11r1wc/common/bin` folder:

```
createManagedServer.py
targetServer.properties
```

3. Check `createManagedServer.py` and modify it for your local environment, if necessary.
4. Modify `targetServer.properties` to supply your WLS installation path and other required information as shown in the following example:

```

## DomainHome chosen for the installation ##
domainHome=/scratch/workdir/mwhome/user_projects/domains/wc_domain/
## OracleHome of the installation location ##
ORACLE_HOME=/scratch/workdir/Feb241515/mwhome/as11r1wc
## Set CONFIG_JVM_ARGS if using adminServerUrl with SSL t3
setenv CONFIG_JVM_ARGS
-Dweblogic.security.SSL.ignoreHostnameVerification=true
-Dweblogic.security.TrustKeyStore=DemoTrust
## AdminServer URL
adminServerUrl=t3://myserver.example.com:7001
## Name of the Managed Server you want to create
mgdServerName=CustomAppServer3
## Username to access the server
user=weblogic
## Password to access the server
password=weblogic
## Port number to be assigned to the new Managed Server
port=9996
#####
## Use serverType "WebCenter" for generic WebCenter custom apps      ##
## or serverType "Portlet" for Portlet producer and bridge custom apps##
#####
serverType=WebCenter
#####
## If you don't want to create a custom schema for the new managed    ##
## server, choose NONE, to use the default WebCenter schema.        ##
## Otherwise, specify the name of the schema you created with the RCU ##
## prior to running the script (creating a new schema is recommended).##
#####
customDS=NONE

```

5. Run the script from your *MW\_HOME/as11r1wc/common/bin* folder:

```
./wlst.sh createManagedServer.py
```

6. Start the newly created WebLogic managed server using the following command:

```

nohup ./startManagedWebLogic.sh custom_server_id http://server_ip_addr:server_
port_num
-Dweblogic.management.username=user_name
-Dweblogic.management.password=password customServer.out &

```

Where:

- *custom\_server\_id* is the name of the new managed server you created (for example, CustomAppServer3).
  - *server\_ip\_addr* is the IP address of the administration server.
  - *server\_port\_num* is the port number of the administration server.
  - *user\_name* is the user name to access the server (for example, weblogic).
  - *password* is the password to access the server (for example, weblogic).
7. Once the managed server is started, check that the schema is registered (the registered MDS schema should appear when you click your WLS domain in Fusion Middleware Control).

You can now continue to deploy your custom WebCenter application as described in [Section 7.1.5, "Deploying a WebCenter Application to a WebLogic Managed Server Instance,"](#) or portlet producer application as described in [Section 12.8, "Deploying Portlet Producer Applications."](#)

## 7.1.4 Creating and Registering the Metadata Service (MDS) Repository

Before you can deploy an application to a managed server, you must first create and register a Metadata Service Repository (MDS) schema for the application on the WebLogic Domain's Administration Server instance.

At deployment time, some of the configuration information and application metadata exported into the .EAR file needs to be imported into a MDS schema for use in the production environment. Importing the metadata occurs automatically during deployment when you select a target metadata schema (as explained in [Section 7.1.5, "Deploying a WebCenter Application to a WebLogic Managed Server Instance"](#)).

---

---

**Caution:** If you deploy using an MDS schema that was created during the WebCenter installation instead of using a custom schema as described in this section, you risk damaging data in those schemas.

---

---

You create the MDS schema using the Repository Creation Utility (RCU). After creating the MDS schema, you then need to register it using either Fusion Middleware Control, or from the command line using WLST.

This section contains the following subsections:

- [Creating an MDS Schema](#)
- [Registering an MDS Schema Using Fusion Middleware Control](#)
- [Registering an MDS Schema Using WLST](#)

### 7.1.4.1 Creating an MDS Schema

Before you deploy an application, you must first create the MDS schema on a database server instance, and then register it on the administration server for the domain to which you're deploying so that the application's metadata can also be deployed.

When following these instructions, be sure to note the MDS schema name and the login credentials for accessing it. You will need this information for subsequent steps in the deployment process.

To create the MDS schema:

1. Navigate to `RCU_HOME/bin` and start the RCU with the following command:

```
rcu
```

The RCU Welcome page displays (see [Figure 7-6](#)).

**Figure 7–6 RCU Welcome Page**

2. Click **Next**.
3. Select **Create** and click **Next**.

The Database Connection Details page displays (see [Figure 7–7](#)).

Figure 7-7 Database Connection Details Page

Repository Creation Utility - Step 2 of 7 : Database Connection Details

**Database Connection Details**

ORACLE 11g  
FUSION MIDDLEWARE

Database Type: Oracle Database

Host Name:   
For RAC database, specify VIP name or one of the Node name as Host name.

Port:

Service Name:

Username:

Password:

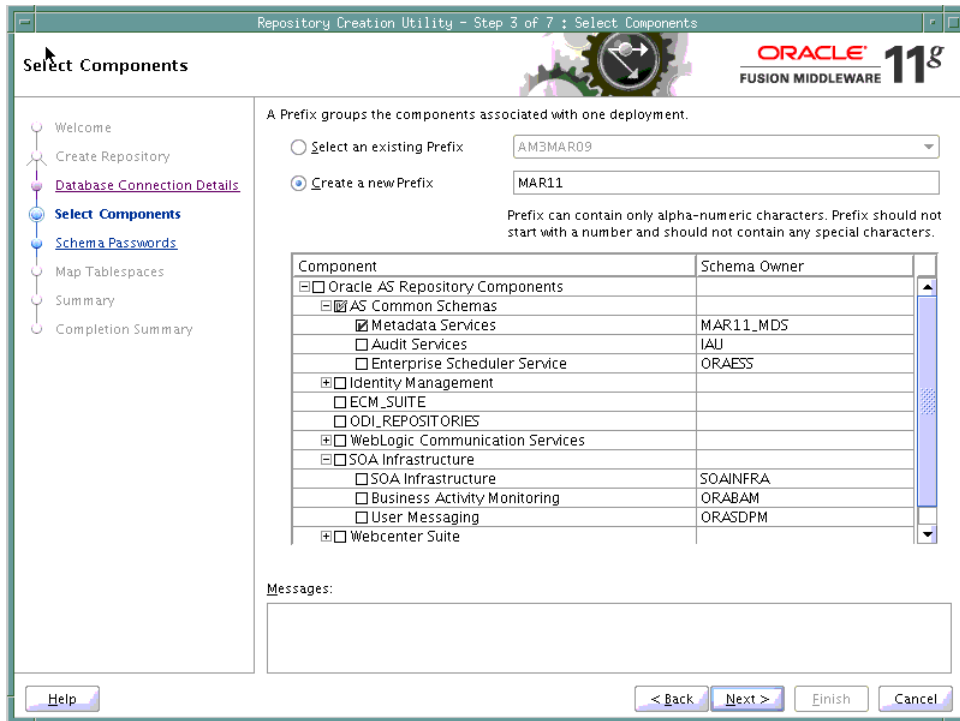
Role: SYSDBA  
One or more components may require SYSDBA role for the operation to succeed.

Messages:

Help < Back Next > Finish Cancel

4. Provide the connection details for the database to which to add the schema by selecting the **Database Type**, entering the **Host Name**, **Port**, **Service Name**, **Username** and **Password** and clicking **Next**.
5. Click **OK** when prompted by the Prerequisites pop-up. The Select Components page displays (see [Figure 7-8](#)).

**Figure 7–8 Select Components Page**



6. Check **Create a New Prefix** and enter a prefix to be prepended to the schema name.
7. Check the **Metadata Services** component. All other components should be left unchecked.
8. Click **Next**, and click **OK** when prompted by the Prerequisites pop-up. The Schema Passwords page displays (see [Figure 7–9](#)).

Figure 7–9 Schema Passwords Page

9. Select how the schema password should be applied, and enter and confirm the password.
10. Click **Next**.
11. On the Map Tablespaces page, click **Next**
12. When prompted to create the tablespaces, click **OK**, and then click **OK** again when the operation is complete.
13. On the Summary page, click **Create** to create the schema.
14. On the Completion Summary page that indicates the successful completion of creating the schema, click **Close**.

#### 7.1.4.2 Registering an MDS Schema Using Fusion Middleware Control

Before you deploy your application, you must first register the new MDS schema with the domain so that applications running on the managed server can access it.

To register an MDS repository using Fusion Middleware Control:

1. Open Fusion Middleware Control and log in to the target domain.  
For information on logging into Fusion Middleware Control, see [Section 6, "Starting Enterprise Manager Fusion Middleware Control."](#)
2. In the Navigation pane, expand the **farm**, then **WebLogic Domain**.
3. Select the domain to which you want to deploy.
4. From the WebLogic Domain menu, select **Metadata Repositories**.

The Metadata Repositories page displays (see [Figure 7–10](#)).

**Figure 7–10 Metadata Repositories Page**

**Metadata Repositories**

You create most Fusion Middleware component schema repositories in a database using the Repository Creation Utility. Metadata Services (MDS) repositories can be created in a database with the Repository Creation Utility or created on disk as file-based repositories. You must register an MDS repository before you can deploy application metadata to the repository.

**Database-Based Repositories**

| Repository Name | Database Type | Database Name | Schema Name        | JNDI Location     |
|-----------------|---------------|---------------|--------------------|-------------------|
| mds-SpacesDS    | Oracle        | wkcdb01       | app1_webcenter_mds | jdbc/mds/SpacesDS |
| mds-owsm        | Oracle        | wkcdb01       | app1_webcenter_mds | jdbc/mds/owsm     |

**File-Based Repositories**

| Repository Name | Directory |
|-----------------|-----------|
| No Repository   |           |

- In the Database-Based Repositories section, click **Register**.

The Register Database-Based Metadata Repository page displays (see [Figure 7–11](#)).

**Figure 7–11 Register Database-based Metadata Repository Page**

Metadata Repositories > Register Metadata Repository

**Register Database-Based Metadata Repository**

A repository stores information used by Application Server components and other applications. A metadata repository must be registered to be operational. A database-based repository is created using the Repository Creation Utility. To register, input database connection information and click Query, then select one of the Metadata Repository and click OK button.

OK Cancel

**Database Connection Information**

Database Type:  Oracle  SQL Server

\* Host Name:

\* Port:

\* Service Name:

Query

\* User Name:

\* Password:

Role: SYSDBA

| Metadata Repository | Is Registered? | Schema Name | Version | Status | Modified Time |
|---------------------|----------------|-------------|---------|--------|---------------|
| No Repository       |                |             |         |        |               |

**Selected Repository**

The selected schema can be registered only if it has not already been registered.

Repository Name:

Schema Password:

- In the Database Connection section, enter the following information:
  - Database** - select the type of database.
  - Host Name** - enter the name of the host.
  - Port** - enter the port number for the database (for example, 1521).
  - Service Name** - enter the service name for the database. The default service name for a database is the global database name, comprising the database name, such as `orcl`, and the domain name, such as `example.com`. In this case, the service name would be `orcl.example.com`.



- **User Name** - enter a username for the database which is assigned the SYSDBA role (for example, *SYS*).
  - **Password** - enter the password for the user.
  - **Role** - select a database role (for example, **SYSDBA**).
7. Click **Query**.
- A table is displayed that lists the schemas and their metadata repositories that are available in the database.
8. Select a repository, then enter the following information:
- **Repository Name** - enter a name for the MDS schema.
  - **Schema Password** - enter the schema password you specified when you created the schema.
9. Click **OK**.
- The repository is registered with the Oracle WebLogic Server domain.

### 7.1.4.3 Registering an MDS Schema Using WLST

You can also use WLST to register a database-based MDS repository from the command line using the `registerMetadataDBRepository` command.

To register an MDS schema using WLST:

1. Start WLST as described in [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)
2. Register the MDS schema using the following command:

```
registerMetadataDBRepository(name='mds_name', dbVendor='db_vendor', host='host_name', port='port_number', dbName='db_name', user='username', password='password', targetServers='target_server')
```

Where:

- *mds\_name* is the name of the MDS schema to register.
- *db\_vendor* is the vendor of the database being used.
- *host\_name* is the host ID of the Database Server.
- *port\_number* is the port number of the Database Server.
- *db\_name* is the name of the database being used to store the MDS.
- *username* is the database schema user name.
- *password* is the database schema password.
- *target\_server* is the name of the target server. For multiple targets, separate the target server names with a comma. Be sure to include the WLS administration server in the list of targets so that the MDS database repository name appears in Deployment plan dialog when you deploy your application to it.

For example, to register the MDS schema `mds1` on the Oracle database `orcl` on the target server `server1` with the host ID of `example.com`, you would use the following command:

```
registerMetadataDBRepository(name='mds1', dbVendor='ORACLE', host='example.com',
```

```
port='1521', dbName='orcl', user='username', password='password',
targetServers='server1', 'AdminServer')
```

## 7.1.5 Deploying a WebCenter Application to a WebLogic Managed Server Instance

Before deploying a custom WebCenter application archive, it is important to make sure that all the required shared libraries are published in the target WebLogic managed server instance.

---

**Note:** Oracle does not recommend deploying custom WebCenter applications to any of the three pre-configured managed servers created during the installation, or to the Administration Server. For custom WebCenter applications created in JDeveloper, follow the process described in [Section 7.1.4, "Creating and Registering the Metadata Service \(MDS\) Repository"](#) and [Section 7.1.3, "Creating and Provisioning a WebLogic Managed Server Instance"](#) to create and provision a new WLS managed server prior to deploying. For portlet producer applications, you can create a new managed server instance, or optionally deploy to the WLS\_Portlet server.

---

Custom WebCenter applications can be deployed in several ways as described in the following sections:

- [Deploying Custom WebCenter Applications Using Oracle JDeveloper](#)
- [Deploying Custom WebCenter Applications Using Fusion Middleware Control](#)
- [Deploying Custom WebCenter Applications Using WLST](#)
- [Deploying WebCenter Applications Using the WLS Administration Console](#)

As explained in [Section 7.1.2, "Creating the .EAR File,"](#) the packaged .EAR file consists of several information artifacts, which includes the application bits, the application configuration, the application metadata, and the portlet customizations.

During the deployment, these information artifacts need to be moved to the right information store in the instance where application is deployed. The target information stores for these artifacts are as described in [Table 7-1](#):

**Table 7-1 Information Artifact Target Stores**

| Information Artifact      | Target Information Store |
|---------------------------|--------------------------|
| Application Bits          | Target Server Instance   |
| Application Configuration | MDS                      |
| Application Metadata      | MDS                      |
| Portlet Customizations    | Target Producer          |

The deployment process automatically migrates the application pieces to right target information store, the location for which is provided by the administrator. Regardless of the tool you choose to deploy, you need to supply the this target information store locations for correct deployment.

Although the application deployment fails if the MDS location is incorrect or not supplied, the application will deploy if the target producer is incorrectly specified. An incorrectly specified target producer means that the portlets are not imported

automatically, so the portlets will not be operational. If that happens, you can remedy it by doing one of the following:

- Edit the portlet producers connections post-deployment using Fusion Middleware Control (see [Section 12.2.1, "Registering a WSRP Producer Using Fusion Middleware Control"](#) and [Section 12.4.1, "Registering an Oracle PDK-Java Producer Using Fusion Middleware Control"](#)) or WLST commands (see [Section 12.2.2, "Registering a WSRP Producer Using WLST"](#) or [Section 12.4.2, "Registering an Oracle PDK-Java Producer Using WLST"](#)), and redeploy the application.
- Export and import the portlet customization using WLST commands (see [Section 16.2, "Exporting and Importing Custom WebCenter Applications for Data Migration"](#)).

### 7.1.5.1 Deploying Custom WebCenter Applications Using Oracle JDeveloper

You can deploy custom WebCenter applications to a WebLogic server instance directly from a development environment using Oracle JDeveloper, provided that you have the necessary credentials to access the WebLogic server. For more information, see the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

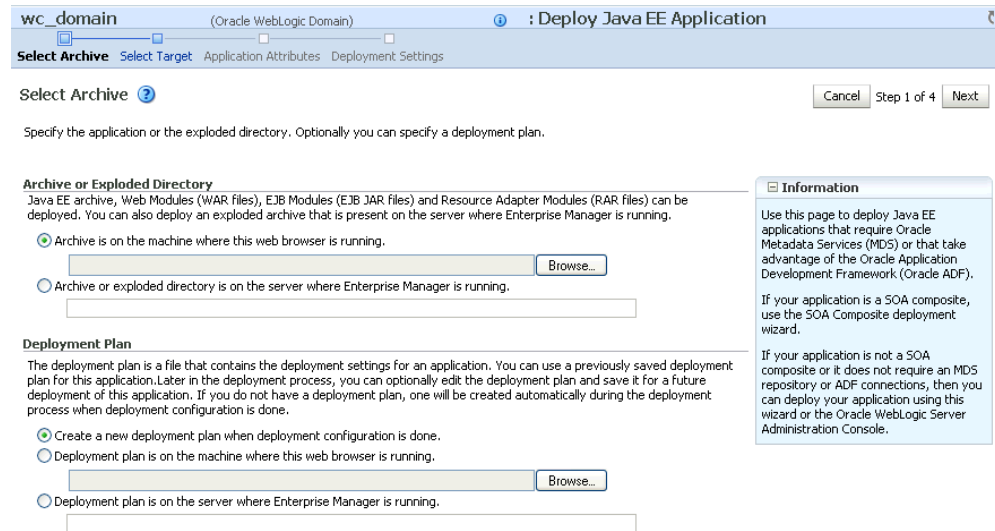
### 7.1.5.2 Deploying Custom WebCenter Applications Using Fusion Middleware Control

When deploying a custom WebCenter application using Fusion Middleware Control you need to know the location of the WebCenter application archive, and whether a deployment plan exists for the application.

To deploy a custom WebCenter application using Fusion Middleware Control:

1. Log in to Fusion Middleware Control.  
See [Section 6.1, "Displaying Fusion Middleware Control Console."](#)
2. In the Navigation pane, expand **WebLogic Domain** and click the domain in which your target managed server was created.
3. From the WebLogic Domain menu, select **Application Deployment > Deploy**.  
The Select Archive page displays (see [Figure 7-12](#)).

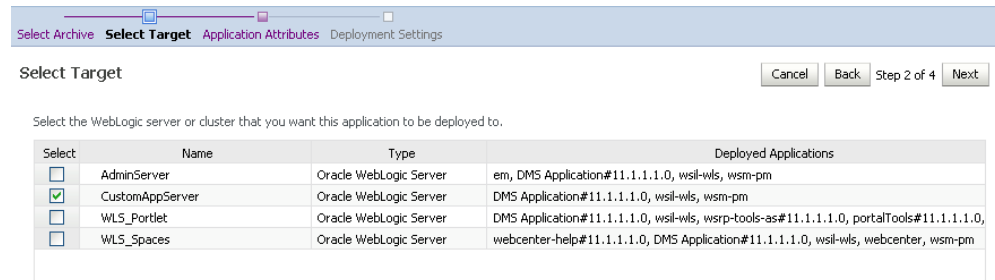
**Figure 7–12 Select Archive Page**



4. In the Archive or Exploded Directory section, do one of the following:
  - Select **Archive is on the machine where this web browser is running** and enter the location of the archive or click **Browse** to find the archive file.
  - Select **Archive or exploded directory is on the server where Enterprise Manager is running** and enter the location of the archive or click **Browse** to find the archive file.
5. In the Deployment Plan section, do one of the following:
  - Select **Create a new deployment plan when deployment configuration is done** to automatically create a new deployment plan after the redeployment process.
  - Select **Deployment plan is on the machine where this web browser is running** and enter the path to the plan or click **Browse** to find the plan.
  - Select **Deployment plan is on the server where Enterprise Manager is running** and enter the path to the plan or click **Browse** to find the plan.
6. Click **Next**.

The Select Target page displays (see [Figure 7–13](#)).

**Figure 7–13 Select Target Page**



7. Select the target server(s) to deploy the application to (see [Section 7.1.5, "Deploying a WebCenter Application to a WebLogic Managed Server Instance"](#) for an overview of selecting the targets) and click **Next**.

The Application Attributes page displays (see [Figure 7-14](#)).

**Figure 7-14 Application Attributes Page**

- Under Target Metadata Repository, click the icon to display the Select metadata repository window, from where you can select the repository for the application, as shown in [Figure 7-15](#). Use the Repository dropdown to select the required repository and then click **OK**.

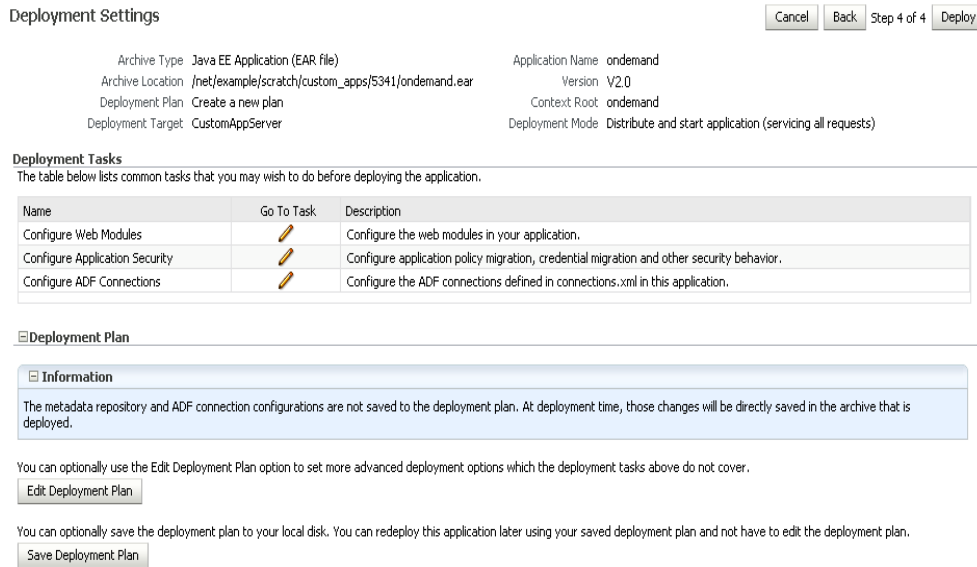
**Note:** The Target Metadata Repository option only displays if the application has metadata to be imported into the MDS repository. This option does not display for a portlet producer application.

**Figure 7-15 Select Metadata Repository Window**

- Enter the name of the partition to use in the repository (typically, the name of the application). Each application must have a unique partition in the repository.
- Click **Next**.

The Deployment Settings page displays (see [Figure 7-16](#)).

**Figure 7–16 Deployment Settings Page**

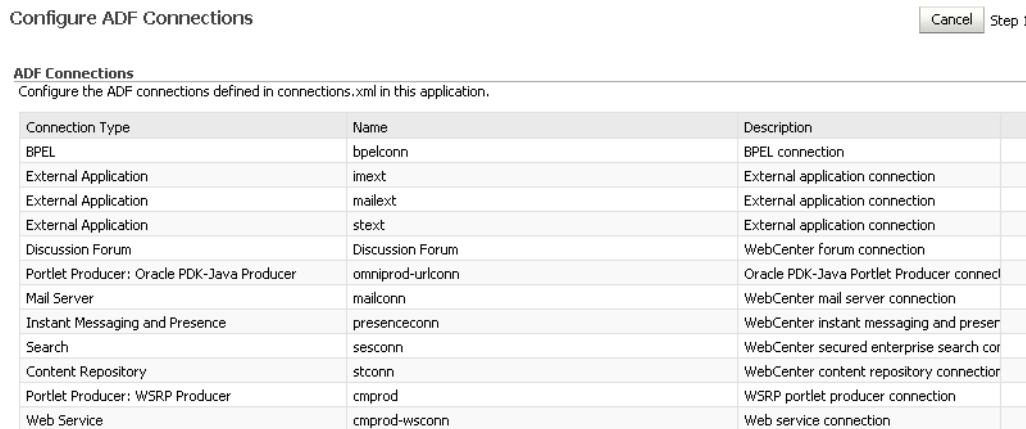


You have now provided the Target MDS location (described in [Section 7.1.5, "Deploying a WebCenter Application to a WebLogic Managed Server Instance"](#)).

11. Click the **edit** icon for Configure ADF Connections to check connection settings associated with the custom WebCenter application.

The Configure ADF Connections page displays (see [Figure 7–17](#)).

**Figure 7–17 Configure ADF Connections Page**



This screenshot shows the Configure ADF Connections page.

\*\*\*\*\*

12. Click the **edit** icon for each connection and check that the connection settings are correct for the target environment (for example, staging or production).

For a Discussion Forum connection (shown in [Figure 7–18](#)), for example, make sure that the URL to the Discussions server, and the user account used to connect to the server are correct for the target environment.

**Figure 7–18 Discussion Forum Connection Settings**

The screenshot shows a window titled "Configure ADF Connection". Inside, the following information is displayed:

- Connection Type: Discussion Forum
- Name: Discussion Forum
- Description: WebCenter forum connection

Below this, under the heading "Connection Details", there are two input fields:

- URL:
- Admin User Name:

At the bottom right of the dialog, there are "OK" and "Cancel" buttons.

For WSRP producers, two connections are shown for each producer: a WSRP Producer and a Web Service connection. Typically only the Web Service connection needs to be changed to the target producer, and this contains four URL endpoints, all of which need to be changed. The WSRP Producer connection only configures proxy settings that can be set independent of the default proxy setting for the application server, if this is required.

If any connections to portlet producers in the .EAR file need to be changed to point to producers in the target deployment environment, it is important to change them here. This ensures the portlet customizations are imported to the target producers as the application starts. For more information, see [Section 7.1.5, "Deploying a WebCenter Application to a WebLogic Managed Server Instance"](#).

---

**Note:** If any target producers are not reachable as the application starts for the first time, the import will not happen. After the portlet producer becomes reachable, restart the application and it will retry the import.

If you do not modify producer connections using the Configure ADF Connections page and they are pointing to incorrect but reachable producer locations (for example, a producer in a development environment), the import of the portlets will occur to the incorrect producers.

To remedy, after deployment use Fusion Middleware Control (see [Section 12.2.1, "Registering a WSRP Producer Using Fusion Middleware Control"](#) and [Section 12.4.1, "Registering an Oracle PDK-Java Producer Using Fusion Middleware Control"](#)) or WLST commands (see [Section 12.2.2, "Registering a WSRP Producer Using WLST"](#) or [Section 12.4.2, "Registering an Oracle PDK-Java Producer Using WLST"](#)) to modify the producer URL endpoint, and then redeploy the application as described in [Section 7.3.2, "Redeploying WebCenter Applications Using Fusion Middleware Control"](#).

---

13. If required, specify additional deployment options such as the Web modules to include in your application or security migration settings.

14. To start the deployment process, click **Deploy**.  
Fusion Middleware Control displays processing messages.
15. Click **Close** in the Deployment Succeeded page.  
The WebCenter application (and its deployment plan) is now deployed on the WebLogic managed server instance.
16. If you restart the WebLogic managed server on which you deployed the application during your Fusion Middleware Control session, refresh the Farm from the Farm menu to update the application status.

---

---

**Note:** When after deploying, you reconfigure connections for custom WebCenter applications, these post-deployment customizations are preserved in the MDS repository and do not need to be set again when you redeploy the application.

---

---

### 7.1.5.3 Deploying Custom WebCenter Applications Using WLST

To deploy a WebCenter application using the WLST command line, WLST must be connected to the Administration Server. You must invoke the `deploy` command on the computer that hosts the administration server.

To deploy a custom WebCenter application using WLST:

1. Start the WLST shell.

For information on starting the WLST shell, see [Section 1.12.3, "Oracle WebLogic Scripting Tool \(WLST\)."](#)

2. Connect to the Administration Server of your WebCenter installation:

```
connect("user_name", "password", "host_id:port")
```

Where:

- `user_name` is the user name to access the Administration server (for example, `weblogic`).
- `password` is the password to access the Administration server (for example, `weblogic`).
- `host_id` is the host ID of the Administration Server (for example, `myserver.example.com`).
- `port` is the port number of the Administration Server (7001 by default)

You should see the following message:

```
Successfully connected to Admin Server 'AdminServer' that belongs to domain 'wc_domain'.
```

3. Retrieve the MDS configuration by running the following command:

```
archive = getMDSArchiveConfig(fromLocation='ear_file_path')
```

where `ear_file_path` is the path and file name of the `.EAR` file you are deploying (for example `/tmp/myEarFile.ear`). For more information, see the `getMDSArchiveConfig` command in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.



- After retrieving the MDS configuration information from the .EAR file, you need to set the proper MDS schema information according to your WebCenter setup (for example, your application might be using a database connection based on a specific schema). To set the MDS schema information, run the following command:

```
archive.setAppMetadataRepository(repository='repository',partition='partition',type='DB',jndi='jndi')
```

Where:

- *repository* is the name of the database schema (for example, `mds-Feb23demo`)
  - *partition* is the individual entity in the repository to allow each application to have its own namespace (for example, `webcenter`).
  - *jndi* is the path and name used to allow access by the application server's other components (for example, `/jdbc/mds/mds-Feb23demo`)
- After setting the MDS repository information, save function the MDS configuration information with the following command:

```
archive.save()
```

- Deploy the custom WebCenter application using the WLST deploy command.

```
deploy(app_name, path, [targets] [stageMode], [planPath], [options])
```

Where:

- *appName* is the name of the custom WebCenter application to be deployed (for example, `composerWLSTApp`).
- *path* is the path to the .EAR file to be deployed (for example, `/tmp/customApp.ear`).
- *targets* specifies the target managed server(s) to which to deploy the application (for example, `CustomAppServer`). You can optionally list multiple comma-separated targets. To enable you to deploy different modules of the application archive on different servers, each target may be qualified with a module name, for example, `module1@server1`. This argument defaults to the server to which WLST is currently connected.
- *[stageMode]* optionally defines the staging mode for the application you are deploying. Valid values are `stage`, `nostage`, and `external_stage`.
- *[planPath]* optionally defines the name of the deployment plan file. The file name can be absolute or relative to the application directory. This argument defaults to the `plan/plan.xml` file in the application directory, if one exists.
- *[options]* is an optional comma-separated list of deployment options, specified as name-value pairs. For more information about valid options, see the WLST deploy command in the Oracle Fusion Middleware WebLogic Scripting Tool Command Reference.

When you see the following message, the application has been successfully deployed and is ready to be accessed:

```
Completed the deployment of Application with status completed
```

---

---

**Note:** Since WLST does not prompt you to modify connections during deployment, the connection information in the .EAR file is used to identify the target producer location in the last start-up. If that location is unreachable, correct the location after deploying the application by bringing up the target producers and restarting the application. Migration of portlet customizations will kick off automatically.

If the producer connections point to incorrect producers (for example, development producers), and those producers are reachable, the migration of portlet customizations will occur using those producers. Since the migration completes, although incorrectly, restarting the application will not automatically restart the migration process.

To remedy this, after deployment, use Fusion Middleware Control (see [Section 12.2.1, "Registering a WSRP Producer Using Fusion Middleware Control"](#) and [Section 12.4.1, "Registering an Oracle PDK-Java Producer Using Fusion Middleware Control"](#)) or WLST commands (see [Section 12.2.2, "Registering a WSRP Producer Using WLST"](#) or [Section 12.4.2, "Registering an Oracle PDK-Java Producer Using WLST"](#)) to modify the producer URL endpoint, and then redeploy the application as described in [Section 7.3.2, "Redeploying WebCenter Applications Using Fusion Middleware Control."](#)

---

---

#### 7.1.5.4 Deploying WebCenter Applications Using the WLS Administration Console

The WLS Administration Console can be used to deploy a custom WebCenter application or a portlet producer application. However, the Console does not offer a means to change ADF connections, including the essential MDS connection. To use the Console to deploy a WebCenter application, the MDS connection in the .EAR file must be already configured to the target deployment repository. Follow steps 1-5 in [Section 7.1.5.3, "Deploying Custom WebCenter Applications Using WLST"](#), then follow the steps below to deploy a custom WebCenter application or portlet producer application using the WLS Administration Console.

---

---

**Note:** For custom WebCenter applications, follow the instructions for creating a new WebLogic managed server as described in [Section 7.1.3, "Creating and Provisioning a WebLogic Managed Server Instance"](#) before deploying. For portlet producer applications, you can optionally create a new WebLogic managed server or deploy to the WLS\_Portlet server.

---

---

To deploy a custom WebCenter or portlet producer application using the WLS Administration Console:

1. Log in to the WLS Administration Console.

For information on logging into the WLS Administration Console, see [Section 1.12.2, "Oracle WebLogic Server Administration Console."](#)

2. In the Domain Structure pane, click **Deployments**.

The Deployments Summary pane displays (see [Figure 7-19](#)).

**Figure 7–19 Deployment Summary Pane**

**Summary of Deployments**

**Control** Monitoring

This page displays a list of Java EE applications and stand-alone application modules that have been installed to this domain. Installed applications and modules can be started, stopped, updated (redeployed), or deleted from the domain by first selecting the application name and using the controls on this page.

To install a new application or module for deployment to targets in this domain, click the Install button.

[Customize this table](#)

**Deployments**

Install Update Delete Start Stop

Showing 1 to 35 of 35 Previous | Next

| <input type="checkbox"/> | Name                                      | State  | Health | Type                   | Deployment Order |
|--------------------------|---|--------|--------|------------------------|------------------|
| <input type="checkbox"/> | adf.oracle.domain(1.0,11.1.1.1.0)         | Active |        | Library                | 100              |
| <input type="checkbox"/> | adf.oracle.domain.webapp(1.0,11.1.1.1.0)  | Active |        | Library                | 100              |
| <input type="checkbox"/> | custom.webcenter.spaces(11.1.1,11.1.1)    | Active |        | Library                | 300              |
| <input type="checkbox"/> | DMS Application (11.1.1.1.0)              | Active | OK     | Web Application        | 190              |
| <input type="checkbox"/> | FMW Welcome Page Application (11.1.0.0.0) | Active | OK     | Web Application        | 150              |
| <input type="checkbox"/> | jpdk                                      | Active | OK     | Enterprise Application | 100              |

- On the Deployment Summary pane, click **Install**.

The Install Application Assistant page displays (see [Figure 7–20](#)).

**Figure 7–20 Install Application Assistant Page**

**Install Application Assistant**

Back Next Finish Cancel

**Locate deployment to install and prepare for deployment**

Select the file path that represents the application root directory, archive file, exploded archive directory, or application module descriptor that you want to install. You can also enter the path of the application directory or file in the Path field.

**Note:** Only valid file paths are displayed below. If you cannot find your deployment files, [upload your file\(s\)](#) and/or confirm that your application contains the required deployment descriptors.

**Path:** /app/oracle/product/fmwhome/user\_projects/domains/webcenter/servers/AdminServer/upload

**Recently Used Paths:**

- /app/oracle/product/fmwhome/user\_projects/domains/webcenter/servers/AdminServer/upload
- /app/oracle/product/fmwhome/webcenteroh/archives/applications
- /app/oracle/product/fmwhome/webcenteroh/webcenter/modules
- /oracle.webcenter.spaces\_11.1.1
- /app/oracle/product/fmwhome/webcenteroh/webcenter/modules
- /oracle.webcenter.framework\_11.1.1

**Current Location:** / app / oracle / product / fmwhome / user\_projects / domains / webcenter / servers / AdminServer / upload

jpdk.ear

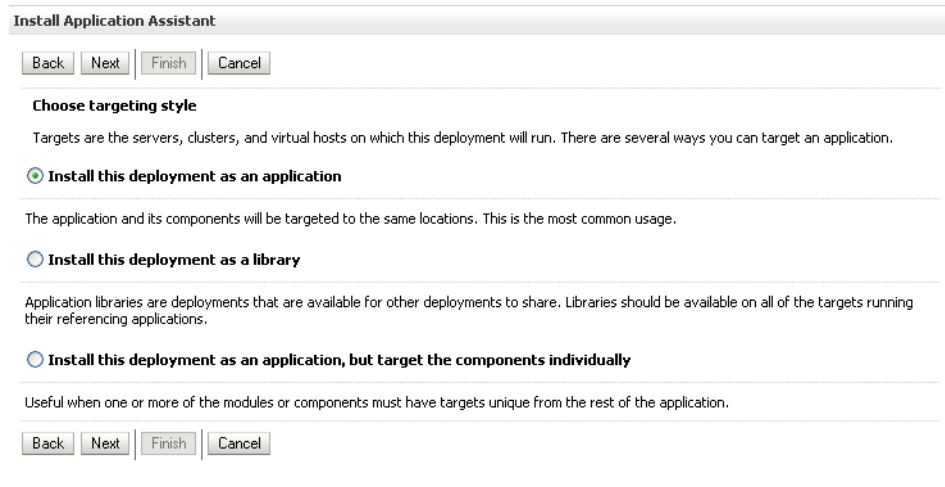
wsrp-samples-as.ear

Back Next Finish Cancel

- Using the Install Application Assistant **Path** field, locate the .EAR file that corresponds to the Web application or portlet producer application you want to install. Select the .EAR file and click **Next**.

Page 2 of the Install Application Assistant page displays (see [Figure 7–21](#)).

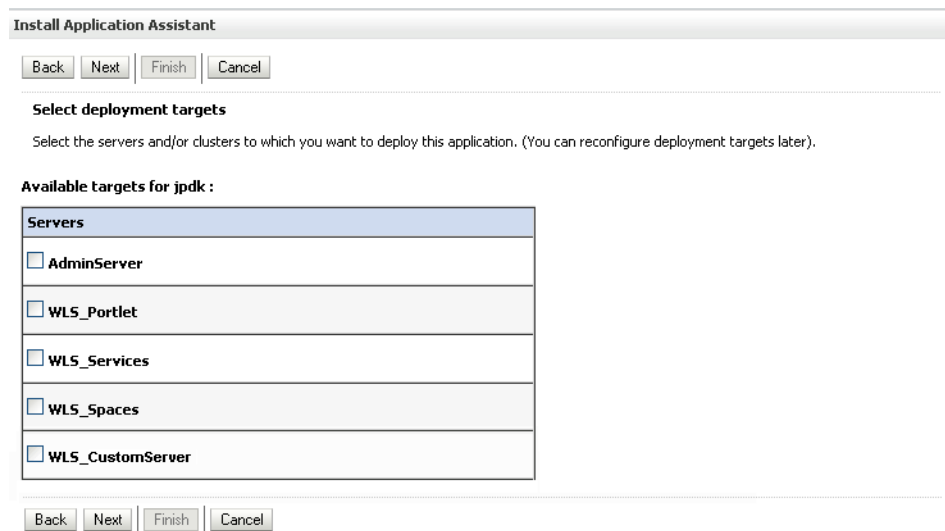
**Figure 7-21 Install Application Assistant - Page 2**



5. Select **Install this deployment as an application** (for both custom WebCenter applications and portlet producers) and click **Next**.

Page 3 of the Install Application Assistant displays (see [Figure 7-22](#)).

**Figure 7-22 Install Application Assistant - Page 3**



6. Select the deployment target to which to deploy the Web application and click **Next**.
7. Review the configuration settings you specified, and click **Finish** to complete the installation.

To change a producer URL after deployment, use Fusion Middleware Control (see [Section 12.2.1, "Registering a WSRP Producer Using Fusion Middleware Control"](#) and [Section 12.4.1, "Registering an Oracle PDK-Java Producer Using Fusion Middleware Control"](#)) or WLST commands (see [Section 12.2.2, "Registering a WSRP Producer Using WLST"](#) or [Section 12.4.2, "Registering an Oracle PDK-Java Producer Using WLST"](#)) to modify the producer URL endpoint, and then redeploy the application as described in [Section 7.3.2, "Redeploying WebCenter Applications Using Fusion Middleware Control."](#)

## 7.1.6 Transporting Customizations Between Environments

You can export and import customizations made to pages, Oracle WebCenter Services, and portlets (PDK-Java and WSRP version 2 producers) of an already deployed application. For more information, see [Chapter 16.2, "Exporting and Importing Custom WebCenter Applications for Data Migration."](#)

## 7.1.7 Configuring WebCenter Applications to Run in a Distributed Environment

For information about configuring your custom WebCenter application to run in a distributed environment, see *Oracle Fusion Middleware Enterprise Deployment Guide for Java EE* and the chapter titled "Active-Active Topologies" in *Oracle Fusion Middleware High Availability Guide*.

## 7.2 Undeploying Custom WebCenter Applications

This section describes how to undeploy a custom WebCenter application or portlet producer application using Fusion Middleware Control, or from the command line using WLST.

---

**Note:** When a custom WebCenter application is undeployed, its application credentials and MDS customizations are kept in anticipation of the application being redeployed to the same domain. If the application will not be redeployed in this domain, or if it is important to reset these back to initial conditions prior to the next deployment, then after undeploying an application you can remove the application's credential map from the Credential Store as described in [Section 7.2.3, "Removing an Application's Credential Map."](#) You can also remove the MDS repository partition as described in "Deleting a Metadata Partition from a Repository" in the *Oracle Fusion Middleware Administrator's Guide*.

---

This section contains the following subsections:

- [Undeploying WebCenter Applications Using Fusion Middleware Control](#)
- [Undeploying WebCenter Applications Using WLST](#)
- [Removing an Application's Credential Map](#)

### 7.2.1 Undeploying WebCenter Applications Using Fusion Middleware Control

This section describes how to undeploy a custom WebCenter application using Fusion Middleware Control.

To undeploy a custom WebCenter application using Fusion Middleware Control:

1. Log in to Fusion Middleware Control.  
See [Section 6.1, "Displaying Fusion Middleware Control Console."](#)
2. From the Navigation pane, expand **Application Deployments**, then click the application that you want to undeploy.
3. From the Application Deployment menu, select **Application Deployment > Undeploy**.
4. On the confirmation page, click **Undeploy**.

5. When the operation completes, click **Close**.

## 7.2.2 Undeploying WebCenter Applications Using WLST

This section describes how to undeploy a custom WebCenter application using WLST.

To undeploy a custom WebCenter application using WLST:

1. Start the WLST shell.

For information on starting the WLST shell, see [Section 1.12.3, "Oracle WebLogic Scripting Tool \(WLST\)."](#)

2. Connect to the Administration Server of your WebCenter installation:

```
connect("user_name", "password", "host_id:7001")
```

Where:

- `user_name` is the user name to access the administration server (for example, `weblogic`).
- `password` is the password to access the administration server (for example, `weblogic`).
- `host_id` is the host ID of the administration server (for example, `myserver.example.com`).

You should see the following message:

```
Successfully connected to Admin Server 'AdminServer' that belongs to domain 'wc_domain'.
```

3. Use the `undeploy` command to undeploy the application:

```
undeploy(app_name, [targets], [options])
```

Where:

- `app_name` is the deployment name for the deployed application.  
`[targets]` is a list of the target servers from which the application will be removed. Optional. If not specified, defaults to all current targets.
- `[options]` is a comma-separated list of deployment options, specified as name-value pairs. Optional. See the `deploy` command for a complete list of options.

## 7.2.3 Removing an Application's Credential Map

When a custom WebCenter application is undeployed, its application credentials are not removed. Consequently, you must manually remove the credential map used for the application after it is undeployed using Fusion Middleware Control.

To remove an application's credentials map using Fusion Middleware Control:

1. Determine the credentials map name used by the application by inspecting the contents of the application's `adf-config.xml` and locating the value for `adfAppUID`. For example:

```
<adf:adf-properties-child
xmlns="http://xmlns.oracle.com/adf/config/properties">
<adf-property name="adfAppUID" value="Veeva-7209"/>
</adf:adf-properties-child>
```

In this case, **Veeva-7209** is the credential map name used by the application.

2. Log in to Fusion Middleware Control.

For information on logging into Fusion Middleware Control, see [Section 6, "Starting Enterprise Manager Fusion Middleware Control."](#)

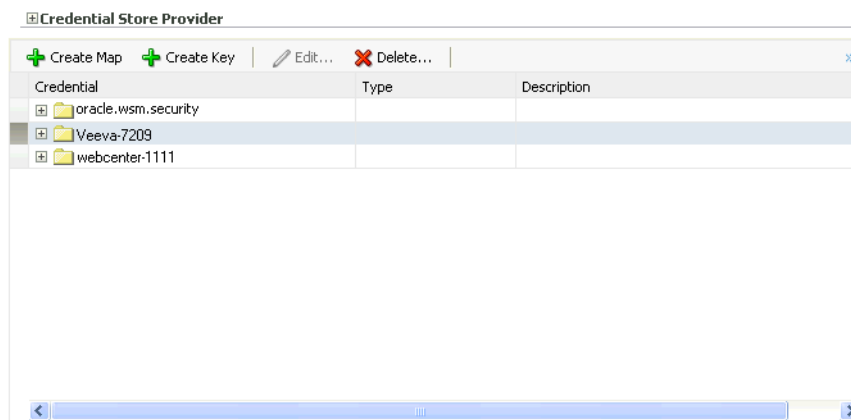
3. In the Navigation pane, expand the WebLogic Domain node and click the target domain (for example, `wc_domain`).
4. From the WebLogic Domain dropdown menu, select **Security > Credentials**.

The Credentials pane displays (see [Figure 7-23](#)).

**Figure 7-23 Credentials Pane**

#### Credentials

A credential store is the repository of security data that certify the authority of entities used by Java 2, J2EE, and ADF applications. Applications can use the Credential Store, a single, consolidated service provider to store and manage their credentials securely.



5. Select the credential map to remove and click **Delete**.
6. Click **Yes** to confirm deleting the credential map.

## 7.3 Redeploying Custom WebCenter Applications

This section describes how to redeploy a custom WebCenter application using Fusion Middleware Control or from the command line using WLST. When you redeploy a new version of an application, you will not be able to change:

- the application's deployment targets
- the application's security model

To change deployment targets or application security settings, you must first undeploy the active version of the application. For information on how to undeploy an application, see [Section 7.2, "Undeploying Custom WebCenter Applications"](#).

This section contains the following subsections:

- [Redeployment Considerations](#)
- [Redeploying WebCenter Applications Using Fusion Middleware Control](#)
- [Redeploying WebCenter Applications Using WLST](#)

## 7.3.1 Redeployment Considerations

In most cases, when redeploying an application, you want to preserve any changes to application data. Three important pieces of information about an application can be altered after deployment:

- Application Configuration -- which includes connection information.
- Application Metadata -- which includes the customizations and personalizations on the application itself, such as those created when user edits a page and adds content to it.
- Portlets Preferences-- which includes customizations and personalizations of the portlet instances.

The following subsections explain how to preserve these three types of information about an application:

- [Preserving Application Configuration](#)
- [Preserving Application Metadata](#)
- [Preserving Portlet Customizations and Personalizations](#)

---

---

**Note:** To preserve application information, you must redeploy using the same MDS partition that was used or created using the initial deployment.

---

---

### 7.3.1.1 Preserving Application Configuration

In most cases, the end-points of services and portlet-producers are different in a test or staging environment than in a production environment. Therefore, when an application is redeployed to a production environment, you must reconfigure the application to work with the production environment services and producers or reuse the configuration used previously. Fusion Middleware facilitates this by storing the configuration information in the MDS repository.

When you deploy the application for the first time, the base document of the application configuration is created in the MDS repository. This configuration is the set of all of the application's connections and their properties that are packaged in the .EAR file. After the deployment, you may need to modify the connections using Fusion Middleware Control or WLST in response to production needs. This reconfiguration creates a layer of customization for the configuration changes in the MDS repository.

When you redeploy the application, the configuration packaged with the application is laid down as the base document, but the customizations to the configuration are preserved. Therefore, the application's redeployment settings will already match the most recent configuration performed.

However, customizations are completely preserved only when there are no changes in the base document. If you redeploy an application where the packaged connection information has changed, the following can be expected:

- A new connection is added to the packaged configuration. The new connection should display without problems.
- A connection has been removed in the packaged configuration. If you configured this connection after the last deployment, then the connection will not display after deployment, you must recreate it.



- A connection property has been changed in the packaged configuration. The customized properties will be used. Connection customizations are managed at the individual connection level, and not at the properties level.

#### 7.3.1.1 Preserving Configuration Across Deployment Using WLST

If you use the WLST to configure the custom WebCenter application, you can easily build a script to remove all the connections and recreate them for the configuration of the production instance. Using this approach, you can always reconfigure an application to the target configuration without worrying about the details in the packaged configuration.

#### 7.3.1.2 Preserving Application Metadata

Application metadata can change post-deployment due to customizations and personalizations done by users at runtime. When you redeploy the application, in most circumstances, you need to preserve this customization and personalization information so that users see exactly what they were seeing before.

Application customizations and personalizations are stored in the MDS repository, and the same rules apply for preserving application metadata as for preserving configuration settings.

When the application is redeployed, the base documents for all application artifacts are replaced with what is packaged in the .EAR file. However, customizations and personalizations are retained. There is no impact to this information unless the base artifact is changed, in which case the same rules apply as for configuration settings, which are:

- If new elements are added to the package, then they will show up as they are.
- If elements are removed from the package, for which customizations or personalizations were created, those personalizations or customizations are ignored.
- If elements are changed, then the effect depends on what exactly is changed, but must be verified.

---

---

**Best Practice Note:** In some cases, you may want to export all customizations and personalizations in a production application instance and import it into a test or staging instance. You can then test the application against those customizations and personalizations to see that the new changes do not have an undesired impact.

---

---

#### 7.3.1.3 Preserving Portlet Customizations and Personalizations

Portlet customizations are packaged with the metadata in the .EAR file. Application startup after deployment kicks off the portlet customization migration to the target producers. The target producers are identified by resolving connection customizations. If you have modified your producer connections prior to redeployment, then those modified connections will be used to identify target producers. Note that if you redeploy an .EAR file with the same checksum (i.e., the same file) as the pre-existing one, portlet customization and personalizations are not overwritten.

### 7.3.2 Redeploying WebCenter Applications Using Fusion Middleware Control

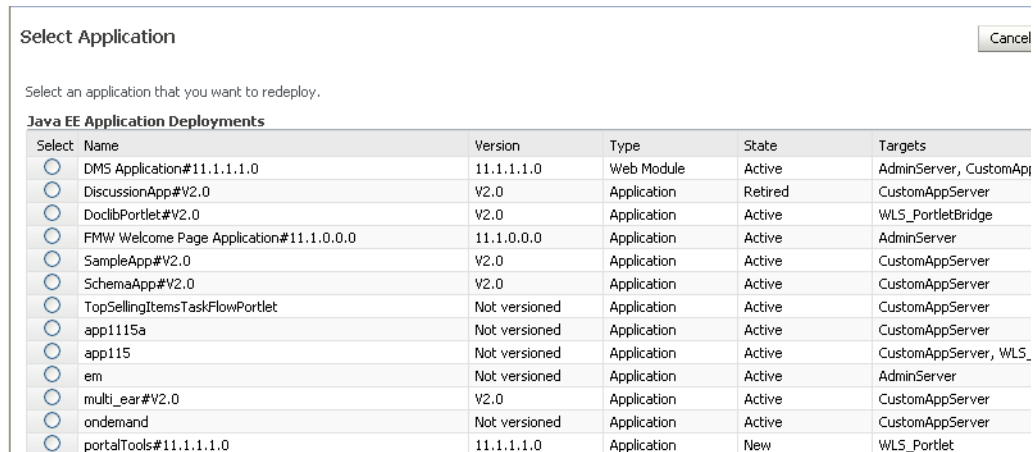
This section describes how to redeploy a custom WebCenter application using Fusion Middleware Control.

To redeploy a custom WebCenter application using Fusion Middleware Control:

1. Log in to Fusion Middleware Control. For more information, see [Section 6.1, "Displaying Fusion Middleware Control Console."](#)
2. From the Navigation pane, expand the farm, then **WebLogic Domain**, and then the domain.
3. Select the server to which to redeploy the application, and then right click and select **Application Deployment - Redeploy** from the menu.

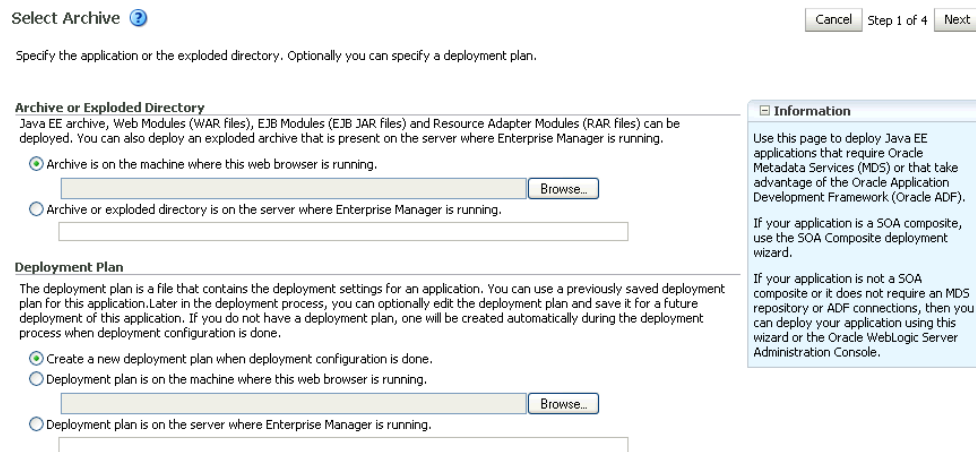
The Select Application page displays (see [Figure 7-24](#)).

**Figure 7-24 Select Application Page**



4. Select the application that you want to redeploy.
5. Click **Next** to display the Select Archive page (see [Figure 7-25](#)).

**Figure 7-25 Select Archive Page**



6. In the Archive or Exploded Directory section, do one of the following:
  - Select **Archive is on the machine where this web browser is running** and enter the location of the archive or click **Browse** to find the archive file.

- Select **Archive or exploded directory is on the server where Enterprise Manager is running** and enter the location of the archive or click **Browse** to find the archive file.
- 7. In the Deployment Plan section, do one of the following:
  - Select **Create a new deployment plan when deployment configuration is done** to automatically create a new deployment plan after the redeployment process.
  - Select **Deployment plan is on the machine where this web browser is running** and enter the path to the plan or click **Browse** to find the plan.
  - Select **Deployment plan is on the server where Enterprise Manager is running** and enter the path to the plan or click **Browse** to find the plan.
- 8. Click **Next**.  
The Application Attributes page displays (see [Figure 7–26](#)).

**Figure 7–26 Application Attributes Page**

Application Attributes Cancel Back Step 3 of


Archive Type Java EE Application (EAR file)  
 Archive Location /net/example/scratch/custom\_apps/5341/ondemand.ear  
 Deployment Plan Create a new plan  
 Deployment Target CustomAppServer

Application Name ondemand  
 Current Version V2.0

**Context Root of Web Modules**

| Web Module   | Context Root |
|--------------|--------------|
| ondemand.war | ondemand     |

**Target Metadata Repository**  
 Select the metadata repository and specify the partition in the repository that the application will be deployed to.

\* Repository Name mds-CustomMDS   
 Repository Type Database  
 \* Partition ondemand

- 9. In the Context Root of Web Modules section, specify the context root for your application if you have not specified it in `application.xml`. The context root is the URI for the web module. Each web module or EJB module that contains web services may have a context root.
- 10. In the Target Metadata Repository section, select the MDS repository and enter the **Partition**.

---

**Caution:** Be careful to use the same repository connection and partition name that you used when you originally deployed the application or all customizations will be lost.

---

- 11. Click **Next**.  
The Deployment Settings page displays (see [Figure 7–27](#)).

**Figure 7–27 Deployment Settings Page**

Deployment Settings
Cancel

Archive Type: Java EE Application (EAR file)

Archive Location: /net/example/scratch/custom\_apps/5341/ondemand.ear

Deployment Plan: Create a new plan

Deployment Target: CustomAppServer

Application Name: ondemand

Version: V2.0

Context Root: ondemand

Deployment Mode: Distribute and start application (servicing all)

**Deployment Tasks**

The table below lists common tasks that you may wish to do before deploying the application.

| Name                           | Go To Task | Description   |
|--------------------------------|------------|---|
| Configure Web Modules          |            | Configure the web modules in your application.  |
| Configure Application Security |            | Configure application policy migration, credential migration and other security behavior. |
| Configure ADF Connections      |            | Configure the ADF connections defined in connections.xml in this application.             |

Deployment Plan

12. On this page, you can perform common tasks before deploying your application, such as configuring connections, or you can edit the deployment plan or save it to a disk. You can:
  - Configure web modules
  - Configure application security for application roles and policies
13. Click the **edit** icon for Configure ADF Connections to check connection settings associated with the custom WebCenter application.

---

**Note:** Editing ADF Connections is only necessary for connections not set after a prior deployment. Any connections configured after a prior deployment will override settings you make during this step.

---

The Configure ADF Connections page displays (see [Figure 7–28](#)).

**Figure 7–28 Configure ADF Connections Page**

Configure ADF Connections
Cancel Step

**ADF Connections**

Configure the ADF connections defined in connections.xml in this application.

| Connection Type                            | Name             | Description                              |
|--|------------------|--|
| BPEL                                       | bpelconn         | BPEL connection                          |
| External Application                       | imext            | External application connection          |
| External Application                       | mailext          | External application connection          |
| External Application                       | stext            | External application connection          |
| Discussion Forum                           | Discussion Forum | WebCenter forum connection               |
| Portlet Producer: Oracle PDK-Java Producer | omniprod-urlconn | Oracle PDK-Java Portlet Producer connect |
| Mail Server                                | mailconn         | WebCenter mail server connection         |
| Instant Messaging and Presence             | presenceconn     | WebCenter instant messaging and preser   |
| Search                                     | sesconn          | WebCenter secured enterprise search cor  |
| Content Repository                         | stconn           | WebCenter content repository connector   |
| Portlet Producer: WSRP Producer            | cmprod           | WSRP portlet producer connection         |
| Web Service                                | cmprod-wsconn    | Web service connection                   |

14. Click the **edit** icon for each connection and check that the connection settings are correct for the target environment (for example, staging or production).  
 For a Discussion Forum connection (shown in [Figure 7–18](#)), for example, make sure that the URL to the discussions server, and the user account used to connect to the server are correct for the target environment.

**Figure 7–29 Discussion Forum Connection Settings**

**Configure ADF Connection**

Connection Type: Discussion Forum  
 Name: Discussion Forum  
 Description: WebCenter forum connection

**Connection Details**

URL:   
 Admin User Name:

OK Cancel

15. If required, specify additional deployment options such as the Web modules to include in your application or security migration settings.
16. Expand Deployment Plan.  
 The Deployment Plan settings display (see [Figure 7–30](#)).

**Figure 7–30 Deployment Settings Page - Deployment Plan Section**

**Deployment Plan**

**Information**

The metadata repository and ADF connection configurations are not saved to the deployment plan. At deployment time, those changes will be directly saved in the archive that is created.

You can optionally use the Edit Deployment Plan option to set more advanced deployment options which the deployment tasks above do not cover.

You can optionally save the deployment plan to your local disk. You can redeploy this application later using your saved deployment plan and not have to edit the deployment plan.

You can edit and save the deployment plan to your local hard drive, if you choose.

17. Click **Redeploy**.
18. When the redeployment completes, click **Close**.

---

**Note:** If you restart the WebLogic managed server on which you deployed the application during your Fusion Middleware Control session, refresh the Farm from the Farm menu to update the application status.

---

### 7.3.3 Redeploying WebCenter Applications Using WLST

To redeploy a custom WebCenter application using the WLST command line, WLST must be connected to the administration server. You must invoke the `redeploy` command on the computer that hosts the administration server.

To redeploy a custom WebCenter application using WLST:

1. Start the WLST shell.

For information on starting the WLST shell, see [Section 1.12.3, "Oracle WebLogic Scripting Tool \(WLST\)."](#)

2. Connect to the administration server of your WebCenter installation:

```
connect("user_name", "password", "host_id:port")
```

Where:

- *user\_name* is the user name to access the administration server (for example, `weblogic`).
- *password* is the password to access the administration server (for example, `weblogic`).
- *host\_id* is the host ID of the administration server (for example, `myserver.example.com`).
- *port* is the port number of the Administration Server (7001 by default).

You should see the following message:

```
Successfully connected to Admin Server 'AdminServer' that belongs to domain 'wc_domain'.
```

3. Use the `redeploy` command to redeploy the application:

```
redeploy(app_name, [planPath], [options])
```

Where:

- *app\_name* is the deployment name for the application to redeploy.
- [*planPath*] Name of the deployment plan file. The filename can be absolute or relative to the application directory. Optional. This argument defaults to the `plan/plan.xml` file in the application directory, if one exists.
- [*options*] is a comma-separated list of deployment options, specified as name-value pairs. Optional. See the `deploy` command for a complete list of options.

---

---

# Starting and Stopping WebCenter Applications

Most WebCenter application configuration changes that you make, through Fusion Middleware Control or using WLST, are not dynamic; you must restart the managed server on which the application is deployed for your changes to take effect. For example, when you add or modify connection details for Web 2.0 services (Announcements, Discussions, Documents, Mail, Instant Messaging and Presence, Search, Worklists) you must restart the application's managed server.

There are several exceptions; portlet producer and external application registration *is* dynamic. Any new portlet producers and external applications that you register are immediately available in your WebCenter application and any changes that you make to existing connections take effect immediately too.

This chapter includes the following sections:

- [Starting Node Manager](#)
- [Starting and Stopping Managed Servers for WebCenter Application Deployments](#)
- [Starting and Stopping WebCenter Spaces](#)
- [Starting and Stopping Custom WebCenter Applications](#)

You perform all start and stop operations from the Oracle WebLogic Server Administration Console too. .

---

---

**Note:** Node Manager must be running before you can start and stop administration servers, managed servers, and WebCenter applications through Fusion Middleware Control or Oracle WebLogic Server Administration Console.

---

---

## Audience

The content of this chapter is intended for Fusion Middleware administrators (users granted the `Admin` or `Operator` role through the Oracle WebLogic Server Administration Console). See also, [Section 1.8, "Understanding Administrative Operations, Roles, and Tools"](#).

## 8.1 Starting Node Manager

Node Manager must be running before you can start and stop administration servers, managed servers, and WebCenter applications through Fusion Middleware Control or Oracle WebLogic Server Administration Console.

To start Node Manager:

1. (First time only). Before starting Node Manager, set the `StartScriptEnabled` property through the `JAVA_OPTIONS` environment variable:  

```
export JAVA_OPTIONS=-DStartScriptEnabled=true
```
2. To start the Node Manager:
  - a. Navigate to `WL_HOME/server/bin`.
  - b. From the command line, enter:  

```
WL_HOME/server/bin> ./startNodeManager.sh
```
3. (First time only) Set the `StartScriptEnabled` property in the `nodemanager.properties` file:
  - a. Open `WL_HOME/common/nodemanager/nodemanager.properties`.  
`nodemanager.properties` does not exist until Node Manager is started for the first time.
  - b. Add the following line:  

```
StartScriptEnabled=true
```

Once this property is set in `nodemanager.properties`, you do not need to define it in the `JAVA_OPTIONS` environment variable.

## 8.2 Starting and Stopping Managed Servers for WebCenter Application Deployments

Most WebCenter configuration changes that you make, through Fusion Middleware Control or using WLST, are not dynamic; you must restart the managed server on which the application is deployed for your changes to take effect.

---

---

**Note:** The only exceptions are portlet producer and external application registration which are both dynamic. New portlet producers and updates to existing producers are immediately available; there is no need to restart the WebCenter application or the managed server. Similarly for external application configuration.

---

---

When you start or restart the managed server, all WebCenter applications deployed on the managed server start automatically (including WebCenter Spaces).

This section describes starting and stopping managed servers through Fusion Middleware Control. See also, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in *Oracle Fusion Middleware Administrator's Guide*.

To start, stop, or restart a managed server through Fusion Middleware Control:

1. Login to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or your custom WebCenter application as follows:
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)

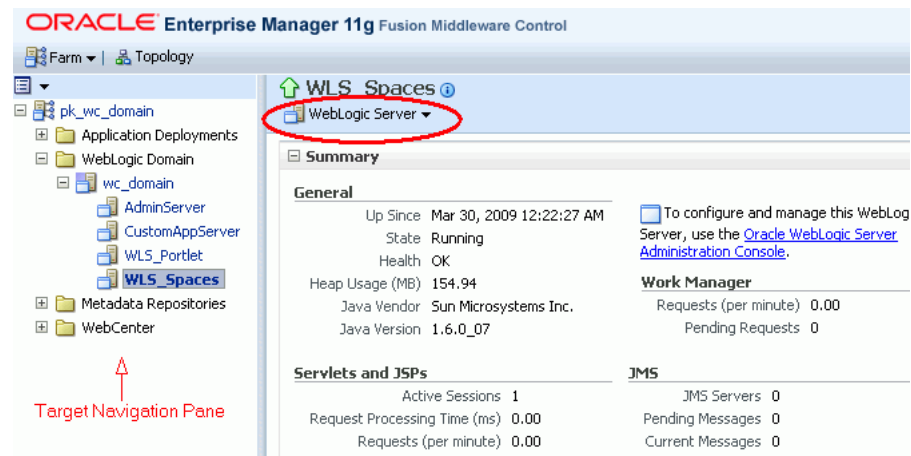


- Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"
2. Navigate to the home page for this application's managed server:
    - For WebCenter Spaces - Find **WebLogic Server** (Related Components section), and then click the name of the managed server. For WebCenter Spaces, this is always *WLS\_Spaces*.
    - For custom WebCenter applications - Find **Deployed On** (Summary section), and then click the name of the managed server.

The home page for the managed server displays (Figure 8–1).

If you know the name of the managed server where your application's is deployed, you can navigate directly to this page if you expand the parent WebLogic Domain in the Target Navigation Pane.

**Figure 8–1 Managed Server Home Page**



3. From the **WebLogic Server** menu:
  - To start the managed server, choose **Control > Start Up**.
  - To stop the managed server, choose **Control > Shut Down**.

Alternatively, right-click the name of the managed server in the Target Navigation Pane to access menu options for the managed server.

## 8.3 Starting and Stopping WebCenter Spaces

It's easy to start, restart, and shut down WebCenter Spaces from Fusion Middleware Control:

- [Starting WebCenter Spaces Using Fusion Middleware Control](#)
- [Stopping WebCenter Spaces Using Fusion Middleware Control](#)

Alternatively, use WLST:

- [Starting WebCenter Spaces Using WLST](#)
- [Stopping WebCenter Spaces Using WLST](#)

---

---

**Note:** You can also start WebCenter Spaces through Oracle WebLogic Server Administration Console.

---

---

### 8.3.1 Starting WebCenter Spaces Using Fusion Middleware Control

Starting WebCenter Spaces makes the application available to its users; stopping it makes it unavailable.

To start WebCenter Spaces through Fusion Middleware Control:

1. In Fusion Middleware Control, navigate to the home page for WebCenter Spaces.  
See [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#).
2. From the main WebCenter menu, choose **WebCenter >Control > Start Up**.  
Alternatively, right-click **WebCenter Spaces (WLS\_Spaces)** in the Target Navigation Pane to access this menu option.  
A progress message displays.
3. Click **Close**.

Note how the application status changes to Up (Green arrow).

### 8.3.2 Starting WebCenter Spaces Using WLST

Use the WLST command `startApplication` to start WebCenter Spaces. For command syntax and detailed examples, see "startApplication" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For WebCenter Spaces, the `appName` argument is always `webcenter`.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

### 8.3.3 Stopping WebCenter Spaces Using Fusion Middleware Control

When you stop WebCenter Spaces no one can use it. Stopping an application does not remove its source files from the server; you can later restart a stopped application to make it available again.

When you stop WebCenter Spaces, the managed server on which WebCenter Spaces is deployed (`WLS_Spaces`) remains available.

To stop a WebCenter Spaces application through Fusion Middleware Control:

1. In Fusion Middleware Control, navigate to the home page for WebCenter Spaces.  
See [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#).
2. From the main menu, choose **WebCenter >Control > Shut Down**.  
Alternatively, right-click **WebCenter Spaces (WLS\_Spaces)** in the Target Navigation Pane to access this menu option.
3. Click **OK** to continue.  
A progress message displays.
4. Click **Close**.

Note how the status changes to Down (Red arrow).

### 8.3.4 Stopping WebCenter Spaces Using WLST

Use the WLST command `stopApplication` to stop WebCenter Spaces. For command syntax and detailed examples, see "stopApplication" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For WebCenter Spaces, the `appName` argument is always `webcenter`.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

## 8.4 Starting and Stopping Custom WebCenter Applications

It's easy to start and shut down custom WebCenter applications from Fusion Middleware Control:

- [Starting Custom WebCenter Applications Using Fusion Middleware Control](#)
- [Stopping Custom WebCenter Applications Using Fusion Middleware Control](#)

Alternatively, use WLST:

- [Starting Custom WebCenter Applications Using WLST](#)
- [Stopping Custom WebCenter Applications Using WLST](#)

### 8.4.1 Starting Custom WebCenter Applications Using Fusion Middleware Control

Starting a custom WebCenter application makes it available to its users; stopping it makes it unavailable.

When you stop a custom WebCenter application, the managed server on which it is deployed remains available.

To start a custom WebCenter application through Fusion Middleware Control:

1. In Fusion Middleware Control, navigate to the home page for the custom WebCenter application.

See [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#).

2. From the Application Deployment menu, choose **Application Deployment >Control > Start Up**.

Alternatively, right-click the name of the custom WebCenter application in the Target Navigation Pane to access this menu option.

A progress message displays.

3. Click **Close**.

Note how the application status changes to Up (Green arrow).

### 8.4.2 Starting Custom WebCenter Applications Using WLST

Use the WLST command `startApplication` to start a custom WebCenter application. For command syntax and detailed examples, see "startApplication" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

### 8.4.3 Stopping Custom WebCenter Applications Using Fusion Middleware Control

When you stop WebCenter Spaces no one can use it. Stopping an application does not remove its source files from the server; you can later restart a stopped application to make it available again.

---

---

**Note:** You can also stop WebCenter Spaces through Oracle WebLogic Server Administration Console.

---

---

To stop a custom WebCenter application:

1. In Fusion Middleware Control, navigate to the home page for the custom WebCenter application.  
  
See [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#).
2. From the main menu, choose **Application Deployment >Control > Shut Down**.  
  
Alternatively, right-click the name of the custom WebCenter application in the Target Navigation Pane to access this menu option.
3. Click **OK** to continue.  
  
A progress message displays.
4. Click **Close**.

Note how the status changes to Down (Red arrow).

### 8.4.4 Stopping Custom WebCenter Applications Using WLST

Use the WLST command `stopApplication` to stop a custom WebCenter application. For command syntax and detailed examples, see "stopApplication" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

---

---

# Setting Application Properties

This chapter includes the following sections:

- [Setting Application Properties for WebCenter Spaces](#)
- [Setting Additional Properties for Custom WebCenter Applications](#)

## Audience

The content of this chapter is intended for Fusion Middleware administrators (users granted the `Admin` role through the Oracle WebLogic Server Administration Console). See also, [Section 1.8, "Understanding Administrative Operations, Roles, and Tools"](#).

## 9.1 Setting Application Properties for WebCenter Spaces

This section includes the following sub sections:

- [Specifying the BPEL Server Hosting WebCenter Spaces Workflows](#)

### 9.1.1 Specifying the BPEL Server Hosting WebCenter Spaces Workflows

WebCenter Spaces uses the BPEL server included with the Oracle SOA Suite to host internal workflows, such as group space membership notifications, group space subscription requests, and so on. To enable workflow functionality inside WebCenter Spaces, a connection to this BPEL server is required.

---

---

**Note:** WebCenter Spaces workflows must be deployed on the SOA managed server that WebCenter Spaces is configured to use. See also, "Back-End Requirements for WebCenter Spaces Workflows" in *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*.

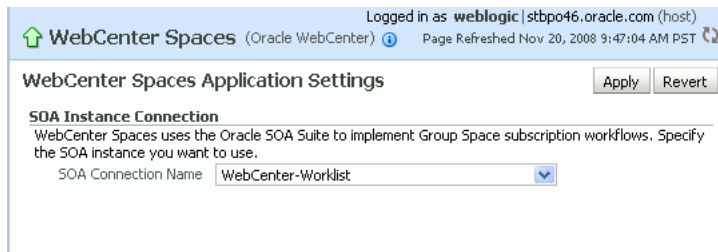
---

---

To configure a connection to the WebCenter Space workflows:

1. Login to Fusion Middleware Control, and navigate to the home page for WebCenter Spaces.  
See [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#).
2. From the **WebCenter** menu, choose **Settings > Application Configuration**.

**Figure 9–1 Choosing the SOA Instance Where WebCenter Spaces Workflows are Deployed**



3. From the **SOA Connection Name** dropdown, choose the name of the connection you require.

The connections on offer are those currently configured for the Worklist service in WebCenter Spaces.

Ensure that you choose the connection that points to the SOA instance in which WebCenter Spaces workflows are deployed. If that connection is not listed you must create it. To define the connection, see [Section 11.5.2.2, "Registering Worklist Connections"](#).

4. Click **Apply**.
5. Restart the managed server on which WebCenter Spaces is deployed to effect this change.

See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments"](#).

## 9.2 Setting Additional Properties for Custom WebCenter Applications

The J2EE Application Deployment home page is your starting place for configuring custom WebCenter application deployments developed with Oracle WebCenter Framework. Just like any other J2EE application, you can configure ADF, MDS, security policies and roles, and so on, from here. To access this page, see [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#).

See also:

- [Section A.4, "Tuning Environment Configuration"](#)
- [Section A.5, "Tuning WebCenter Application Configuration"](#)
- [Section A.6, "Tuning Back-End Component Configuration"](#)

---

---

## Managing Content Repositories

Oracle WebCenter enables content integration through:

- Content Repository data controls, which enable read-only access to a content repository, and maintain tight control over the way the content displays in the application.
- The Documents service, which enables users to view and manage documents in your organization's content repositories.

This chapter describes how to configure and manage content repositories used by WebCenter Spaces and custom WebCenter applications deployed on Oracle WebLogic Server. For more information about managing and including content in WebCenter applications, see:

- "Integrating Content" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*, which describes how to include content in a custom WebCenter application at design time using JCR data controls.
- "Integrating the Documents Service" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*, which describes how to integrate the Documents service in a custom WebCenter application at design time, creating a user-friendly interface to manage documents at runtime.
- "Working with the Documents Service" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*, which describes how to work with the Documents service and task flows at runtime in WebCenter Spaces and custom WebCenter applications.

---

---

**Note:** Any content repository configuration changes that you make through Fusion Middleware Control or using WLST are not dynamic; you need to restart the managed server on which the WebCenter application is deployed for your changes to take effect. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments"](#).

---

---

This chapter contains the following subsections:

- [What You Should Know About Content Repository Connections](#)
- [Content Repository Prerequisites](#)
- [Registering Content Repositories](#)
- [Changing the Active \(or Default\) Content Repository Connection](#)
- [Modifying Content Repository Connection Details](#)

- [Deleting Content Repository Connections](#)
- [Setting Connection Properties for the WebCenter Spaces Content Repository](#)
- [Testing Content Repository Connections](#)
- [Changing the Maximum File Upload Size](#)

### **Audience**

The content of this chapter is intended for Fusion Middleware administrators (users granted the `Admin` or `Operator` role through the Oracle WebLogic Server Administration Console). See also, [Section 1.8, "Understanding Administrative Operations, Roles, and Tools"](#).

## **10.1 What You Should Know About Content Repository Connections**

WebCenter users need to store, publish, and share files. The Documents service provides content management and storage capabilities for WebCenter applications, including content upload, file and folder creation and management, file check out, versioning, and so on. To do this, the Documents service requires at least one content repository connection (WebCenter applications can support multiple content repository connections) to be made active:

- **WebCenter Spaces** - In WebCenter Spaces, every group space and personal space has its own document folder, unique to its parent space. The back-end service providing this functionality is Oracle Content Server. When a content repository is made active (see [Section 10.4, "Changing the Active \(or Default\) Content Repository Connection"](#)), it becomes the default content repository and additional properties become available for configuration. WebCenter Spaces *requires* the default content repository to be Oracle Content Server. Additionally, administrators may connect WebCenter Spaces to other content repositories that WebCenter Spaces may use.
- **Other WebCenter applications** - When a content repository is made active (see [Section 10.4, "Changing the Active \(or Default\) Content Repository Connection"](#)), Documents service task flows use that content repository in instances where no specific connection details are provided. There is no particular requirement on the default content repository used.

When Oracle Content Server is the content repository (required for WebCenter Spaces), the identity store configured for the Documents service must be LDAP-based, not a file-based jazn store, and Oracle Content Server must be connected to that same identity store.

Just like other service connections, post-deployment, content repository connections are registered and managed through Fusion Middleware Control or using the WLST command-line tool. Connection information is stored in configuration files and in the MDS repository. For more information, see [Section 1.3.4, "Oracle WebCenter Configuration Considerations"](#).

Always use Fusion Middleware Control or WLST command-line tool to review and configure back-end services for WebCenter applications. Any changes that you make to WebCenter applications, post-deployment, are stored in the Oracle Metadata Service (MDS) repository as customizations.

Once connection details are defined, WebCenter users can expose the content of the connected content repositories through several ADF Faces components, such as `<af:image>`, `<af:inlineFrame>`, and `<af:goLink>`, and built-in Documents service task flows (Documents, Document List Viewer, and Recent Documents). For



more information, see "Working with Page Content" and "Working with the Documents Service" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

## 10.2 Content Repository Prerequisites

Oracle WebCenter's support of the JCR 1.0 open document standard enables integration with multiple back-end content stores. Oracle WebCenter supports the following content repositories: Oracle Content Server, Oracle Portal, and the file system.

---



---

**Caution:** File system connections *must not* be used in production or enterprise application deployments. This feature is provided for development purposes only

---



---

- [Oracle Content Server Prerequisites](#)
- [Oracle Portal Prerequisites](#)
- [File System Prerequisites](#)

### 10.2.1 Oracle Content Server Prerequisites

This section contains the following subsections:

- [Oracle Content Server - Installation](#)
- [Oracle Content Server - Configuration](#)
- [Oracle Content Server - Security Considerations](#)
- [Oracle Content Server - Limitations in WebCenter](#)

#### 10.2.1.1 Oracle Content Server - Installation

Oracle Content Server 10.1.3.4.1 installation is integrated with Oracle WebCenter installation. Alternatively, you can choose to install Oracle Content Server separately without installing Oracle WebCenter components, provided certain configuration requirements are satisfied. For information about installing Oracle Content Server, see the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*.

#### 10.2.1.2 Oracle Content Server - Configuration

After installing Oracle Content Server, you must configure the server to use the same LDAP-based identity store that Oracle WebCenter has been configured to use. You can optionally configure Oracle Content Server for using full-text search and index and Secure Socket Layer (SSL) for secure identity propagation. [Table 10–1](#) lists the various configuration tasks and specifies whether these tasks are mandatory or optional.

**Table 10–1 Oracle WebCenter-Specific Postinstallation Configuration Tasks for Oracle Content Server**

| Task  | Mandatory/Optional |
|---|--------------------|
| <a href="#">Configuring the Identity Store</a>            | Mandatory          |
| <a href="#">Enabling Full-Text Searching and Indexing</a> | Optional           |
| <a href="#">Configuring Secure Socket Layer (SSL)</a>     | Optional           |

##### 10.2.1.2.1 Configuring the Identity Store

Both Oracle Content Server and Oracle WebCenter must be configured to use the same LDAP-based identity store. By default, Oracle Content Server is not set up with an LDAP-based identity store.

To configure Oracle Content Server to use an LDAP-based identity store:

1. Start the Oracle Content Server console and log on as an administrator.
2. From the **Administration** menu, select **Providers**.
3. In the **Create a New Provider** section, for the **ldapuser** provider type, click **Add** in the **Action** column. (Figure 10-1)

**Figure 10-1** *Creating a New Provider*

**Create a New Provider**

| Provider Type       | Description                            | Action              |
|---------------------|--|---------------------|
| <b>outgoing</b>     | Configuring an outgoing provider.      | <a href="#">Add</a> |
| <b>database</b>     | Configuring a database provider.       | <a href="#">Add</a> |
| <b>incoming</b>     | Configuring an incoming provider.      | <a href="#">Add</a> |
| <b>preview</b>      | Configuring a preview provider.        | <a href="#">Add</a> |
| <b>ldapuser</b>     | Configuring an LDAP user provider.     | <a href="#">Add</a> |
| <b>httpoutgoing</b> | Configuring an HTTP outgoing provider. | <a href="#">Add</a> |

4. Specify details for the LDAP provider. You must specify the following details: provider name, provider description, provider class, source path, LDAP server, LDAP suffix, and LDAP port. You may also specify the LDAP admin user and password. (Figure 10-2)

The LDAP server details that you enter must be of the server that Oracle WebCenter is configured to use.

---



---

**Note:** Set the **Default Network Accounts** field to #none. Do not set any default role because all user security information is stored using the extended user attribute component of Oracle Content Server. You can set the **Role Prefix** and **Account Prefix** fields to any path that does not exist on the LDAP server.

---



---

**Figure 10–2 Specifying Details of a New LDAP Provider**

| Add LDAP Provider                  |   |
|------------------------------------|---|
| Provider Name                      | <input type="text"/>  |
| Provider Description               | <input type="text"/>  |
| Provider Class                     | <input type="text" value="intradoc.provider.LdapUserProvider"/> |
| Connection Class                   | <input type="text" value="intradoc.provider.LdapConnection"/>   |
| Configuration Class                | <input type="text"/>  |
| Source Path                        | <input type="text"/>  |
| LDAP Server                        | <input type="text"/>  |
| LDAP Suffix                        | <input type="text"/>  |
| LDAP Port                          | <input type="text" value="389"/>                                |
| Number of connections              | <input type="text" value="5"/>                                  |
| Connection timeout                 | <input type="text" value="10"/>                                 |
| Priority                           | <input type="text" value="1"/>                                  |
| Credential Map                     | <input type="text"/>  |
| Use Netscape SDK                   | <input checked="" type="checkbox"/>                             |
| Use SSL                            | <input type="checkbox"/>  |
| Use Group Filtering                | <input type="checkbox"/>  |
| Use Full Group Names               | <input type="checkbox"/>  |
| Account Permissions Delimiter      | <input type="text" value="-"/>                                  |
| Default Network Roles              | <input type="text"/>  |
| Default Network Accounts           | <input type="text" value="#none"/>                              |
| Role Prefix                        | <input "="" type="text" value="OU=Roles,OU=UCM,OU=("/>          |
| Depth                              | <input type="text" value="1"/>                                  |
| <input type="button" value="Add"/> |   |

5. Click the **Add** button to add the LDAP provider.
6. Click the **Test** link on the main providers page to verify that the new LDAP connection works fine.

#### 10.2.1.2.2 Enabling Full-Text Searching and Indexing

By default, the database used by Oracle Content Server is set up to provide metadata-only searching and indexing capabilities. However, you can modify the default configuration of SQL Server, Oracle, and DB2 to additionally support full-text searching and indexing. Configuring full-text searching and indexing capabilities is optional, but advisable.

For information about enabling full-text searching and indexing, see the "Setting Up Database Search and Indexing" appendix in the *Content Server Installation Guide for Microsoft Windows* or *Content Server Installation Guide for UNIX* available at:

[http://download.oracle.com/docs/cd/E10316\\_01/owc.htm](http://download.oracle.com/docs/cd/E10316_01/owc.htm)

**10.2.1.2.3 Configuring Secure Socket Layer (SSL)** If Oracle Content Server and the WebCenter application in which you intend to create a repository connection are not on the same system or the same trusted private network, then identity propagation is not secure. To ensure security, you must configure SSL on Oracle Content Server.

Configuration of SSL on Oracle Content Server involves the following tasks:

- [Configuring a Keystore and Key on the Client Side](#)
- [Configuring a Keystore and Key on the Server Side](#)

- [Verifying Signatures of Trusted Clients](#)
- [Securing Identity Propagation](#)

You can also refer to "SSL Properties" in *Content Integration Suite Administration Guide* available at [http://download.oracle.com/docs/cd/E10316\\_01/ouc.htm](http://download.oracle.com/docs/cd/E10316_01/ouc.htm). Perform these procedures if you use self-signed certificates.

In a production environment, it is recommended that you use real certificates. For information about how to configure keystores when using real certificates, see the "Using Security Providers" chapter in the *Security Providers Component Administration Guide* available at [http://download.oracle.com/docs/cd/E10316\\_01/ouc.htm](http://download.oracle.com/docs/cd/E10316_01/ouc.htm).

For more information about configuration for SSL, see [Section 14.6, "Configuring WebCenter Applications and Components to Use SSL"](#).

### Configuring a Keystore and Key on the Client Side

To configure a keystore on the WebCenter application (client) side:

1. In your development environment, go to *JDEV\_HOME*/jdk/bin and open the command prompt.
2. Generate the client keystore by running the following keytool command:

```
keytool -genkey -keyalg RSA -validity 5000 -alias Client private key alias
-keystore client-keystore.jks
-dname "cn=client" -keypass Private key password -storepass KeyStore password
```

3. To verify that the keys have been correctly created, you can optionally run the following keytool command:

```
keytool -list -keystore client-keystore.jks -storepass KeyStore password
```

4. To use the key, sign it by running the following keytool command:

```
keytool -selfcert -validity 5000 -alias Client private key alias -keystore
client-keystore.jks
-keypass Private key password -storepass KeyStore password
```

5. Export the client public key by running the following keytool command:

```
keytool -export -alias Client private key alias -keystore client-keystore.jks
-file client.pubkey -keypass Private key password -storepass KeyStore password
```

### Configuring a Keystore and Key on the Server Side

To configure a keystore on the Oracle Content Server side:

1. In the same development environment, go to *JDEV\_HOME*/jdk/bin and open the command prompt.
2. Generate the server keystore by running the following keytool command:

```
keytool -genkey -keyalg RSA -validity 5000 -alias Server public key alias
-keystore server-keystore.jks -dname "cn=server" -keypass Private server key
password -storepass KeyStore password
```

3. To verify that the key has been correctly created, run the following keytool command:

```
keytool -list -keystore server-keystore.jks -keypass Server private key
password -storepass KeyStore password
```

4. To use the key, sign it by running the following keytool command:

```
keytool -selfcert -validity 5000 -alias Server public key alias -keystore
server-keystore.jks
-keypass Private server key password -storepass KeyStore password
```

5. Export the server public key to the server keystore by running the following keytool command:

```
keytool -export -alias Server public key alias -keystore server-keystore.jks
-file server.pubkey -keypass Server private key password -storepass KeyStore
password
```

### Verifying Signatures of Trusted Clients

To verify signatures of trusted clients, import the client public key into the server keystore:

1. In your development environment, go to *JDEV\_HOME/jdk/bin* and open the command prompt.
2. To verify the signature of trusted clients, import the client's public key in to the server keystore by running the following keytool command:

```
keytool -import -alias Client public key alias -file client.pubkey -keystore
server-keystore.jks -keypass Private server key password -storepass KeyStore
password
```

3. Import the server public key into the client keystore by running the following keytool command:

```
keytool -import -alias Server public key alias -file server.pubkey -keystore
client-keystore.jks -keypass Private key password -storepass KeyStore password
```

When the tool prompts you if the key is self-certified, you must enter *Yes*.

[Example 10-1](#) shows a sample output that is generated after this procedure is completed successfully.

#### Example 10-1 Sample Output Generated by the Keytool

```
[user@server]$ keytool -import -alias client -file client.pubkey
-keystore server-keystore.jks -keypass Server private key password -storepass
Keystore password
Owner: CN=client
Issuer: CN=client
Serial number: serial number, for example, 123a19cb
Valid from: Date, Year, and Time until: Date, Year, and Time
Certificate fingerprints:
...
Trust this certificate? [no]: yes
Certificate was added to keystore.
```

### Securing Identity Propagation

To secure identity propagation, you must configure SSL on Oracle Content Server.

1. Log on to Oracle Content Server as an administrator.
2. From **Administration**, choose **Providers**.
3. On the Create a New Provider page, click **Add** for **sslincoming**.
4. On the Add Incoming Provider page, in **Provider Name**, enter a name for the provider, for example, *sslincomingprovider*.

When the new provider is set up, a directory with the provider name is created as a subdirectory of the `CONTENT_SERVER_HOME/data/providers` directory.

5. In **Provider Description**, briefly describe the provider, for example, `SSL Incoming Provider` for securing the Content Server.
6. In **Provider Class**, enter the class of the sslincoming provider, for example, `idc.provider.ssl.SSLSocketIncomingProvider`.

---

**Note:** You can add a new SSL keepalive incoming socket provider or a new SSL incoming socket provider. Using a keepalive socket improves the performance of a session and is recommended for most implementations.

---

7. In **Connection Class**, enter the class of the connection, for example, `idc.provider.KeepaliveSocketIncomingConnection`.
8. In **Server Thread Class**, enter the class of the server thread, for example, `idc.server.KeepaliveIdcServerThread`.
9. In **Server Port**, enter an open server port, for example, `5555`.
10. Select the **Require Client Authentication** checkbox.
11. In **Keystore password**, enter the password to access the keystore.
12. In **Alias**, enter the alias of the keystore.
13. In **Alias password**, enter the password of the alias.
14. In **Truststore password**, enter the password of the trust store.
15. Click **Add**.

The new incoming provider is now added.

16. Go to the new provider directory that was created in step 4.
17. To specify truststore and keystore, create a file named `sslconfig.hda`.
18. Copy the server keystore to the server.
19. Configure the `sslconfig.hda` file. [Example 10–2](#) shows how the `.hda` file should look after you include the truststore and keystore information.

**Example 10–2 Sample `sslconfig.hda` File**

```
@Properties LocalData
TruststoreFile=/tmp/ssl/server_keystore
KeystoreFile=/tmp/ssl/server_keystore
@end
```

### 10.2.1.3 Oracle Content Server - Security Considerations

To secure identity propagation, you must configure SSL on Oracle Content Server. This is required when Oracle Content Server and your WebCenter application are not on the same system or the same trusted private network. For information, see [Section 10.2.1.2.3, "Configuring Secure Socket Layer \(SSL\)."](#)

### 10.2.1.4 Oracle Content Server - Limitations in WebCenter

None.

## 10.2.2 Oracle Portal Prerequisites

This section contains the following subsections:

- [Oracle Portal - Installation](#)
- [Oracle Portal - Configuration](#)
- [Oracle Portal - Security Considerations](#)
- [Oracle Portal - Limitations in WebCenter](#)

### 10.2.2.1 Oracle Portal - Installation

For information on installing Oracle Portal, see *Oracle Fusion Middleware Installation Guide for Oracle Portal, Forms, Reports and Discoverer*.

### 10.2.2.2 Oracle Portal - Configuration

Oracle Portal must be up-to-date with all the latest patches. For additional information about patches, see the product release notes. See also *Oracle Fusion Middleware Administrator's Guide for Oracle Portal*.

### 10.2.2.3 Oracle Portal - Security Considerations

None.

### 10.2.2.4 Oracle Portal - Limitations in WebCenter

Oracle Portal integration with Oracle WebCenter is read-only. It is not possible to create content in the portal from Oracle WebCenter.

You can expose Oracle Portal pages in WebCenter through the Federated Portal Adapter by publishing them as portlets in Oracle Portal. The following are not returned by the Federated Portal Adapter, and thus are not visible in Oracle WebCenter:

- Seeded page groups:
  - Oracle Portal repository.
  - Oracle Portal design-time pages.
- Pages of the following types:
  - Mobile.
  - URL.
  - Navigation pages.
- Items of the following types:
  - Navigation items.
  - PLSQL items.
  - Portlet.
  - Portlet instance.
  - URL items.
  - Mobile items.
  - Page links.
  - Item links.

- Items defined as:
  - Expired.
  - Hidden.

### 10.2.3 File System Prerequisites

This section contains the following subsections:

- [File System - Security Considerations](#)
- [File System - Limitations in WebCenter](#)

#### 10.2.3.1 File System - Security Considerations

All operations are executed as the system user under which the JVM is running and therefore inherit its permissions.

#### 10.2.3.2 File System - Limitations in WebCenter

File system connections must not be used in production or enterprise application deployments, and search capabilities are limited and slow due to the absence of an index. This feature is provided for development purposes only.

## 10.3 Registering Content Repositories

This section contains the following subsections:

- [Registering Content Repositories Using Fusion Middleware Control](#)
- [Registering Content Repositories Using WLST](#)

### 10.3.1 Registering Content Repositories Using Fusion Middleware Control

To register a content repository:

1. Log in to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application:
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)
  - [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#)
2. Do one of the following:
  - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings > Service Configuration**.
  - For custom WebCenter applications - From the **Application Deployment** menu, choose **WebCenter > Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, select **Content Repository**.
4. To connect to a new content repository, click **Add** ([Figure 10-3](#)).



**Figure 10–3 Configuring Content Repository Connections**

| Manage Content Repository Connections |                       |                   |
|---------------------------------------|-----------------------|-------------------|
| + Add   Edit   X Delete               |                       |                   |
| Name                                  | Repository Type       | Active Connection |
| pktest2                               | Oracle Content Server |                   |

5. Enter a unique name for this connection, specify the content repository type, and indicate whether this connection is the active (or default) connection for the application. See [Table 10–2](#).

**Table 10–2 Manage Content Repository Connections**

| Field           | Description  |
|-----------------|--|
| Connection Name | Enter a unique name for this content repository connection. The name must be unique (across all connection types) within the WebCenter application.  |
| Repository Type | <p>Choose the type of repository you want to connect to. Select one of the following:</p> <ul style="list-style-type: none"> <li>■ <b>Oracle Content Server</b> - an Oracle Universal Content Management repository. See also, <a href="#">Oracle Content Server Prerequisites</a>.</li> <li>■ <b>Oracle Portal</b> - an Oracle Portal content repository. See also, <a href="#">Oracle Portal Prerequisites</a>.</li> <li>■ <b>File System</b> - a computer file system. See also, <a href="#">File System Prerequisites</a>.</li> </ul> <p><b>Caution:</b> File system connections <i>must not</i> be used in production or enterprise application deployments. This feature is provided for development purposes only.</p> <p>(WebCenter Spaces) If you are setting up the backend content repository for WebCenter Spaces, that is, the repository used by WebCenter Spaces to store group space and personal space documents, you must select <b>Oracle Content Server</b>.</p> |

**Table 10–2 (Cont.) Manage Content Repository Connections**

| Field             | Description   |
|-------------------|---|
| Active Connection | <p>Select to make this the <i>default</i> content repository for your WebCenter application.</p> <p>You can connect your WebCenter application to multiple content repositories; all connections are used. One connection must be designated the <i>default</i> (or active) connection. Do one of the following:</p> <ul style="list-style-type: none"> <li>■ For WebCenter Spaces:                     <p>Select to make this the <i>active connection</i>, that is, the back-end repository that WebCenter Spaces uses to store group space and personal space documents. The active connection must be to an Oracle Content Server.</p> <p>If this is the <i>active connection</i> for WebCenter Spaces, some additional configuration is required -- see <a href="#">Table 10–3, "Content Repository Connection - WebCenter Spaces Repository Details"</a>.</p> </li> <li>■ For other WebCenter applications:                     <p>Select to make this the <i>active connection</i>; that is, the default connection for Documents service task flows (Documents, Document List Viewer, and Recent Documents). When no specific connection details are provided for these task flows, this default (active) connection is used.</p> </li> </ul> <p>Deselecting this option does not disable the content repository connection. If a content repository is no longer required, you must delete the connection.</p> |

6. (For the active connection in WebCenter Spaces only.) Enter additional details for the WebCenter Spaces repository (see [Table 10–3](#)).

**Table 10–3 Content Repository Connection - WebCenter Spaces Repository Details**

| Field                   | Description   |
|-------------------------|---|
| Administrator User Name | <p>Enter the user name of the content repository administrator.</p> <p>For example: <code>sysadmin</code></p> <p>Administrative privileges are required for this connection so that operations can be performed on behalf of WebCenter users.</p>   |
| Spaces Root             | <p>Enter the root folder under which group space content is stored. Specify a folder that does not yet exist and is unique across applications. Use the format: <code>/foldername</code>. This name cannot be the same as the Application Name.</p> <p>For example: <code>/MyWebCenterSpaces</code></p> <p>If it does not already exist, the folder specified is automatically created when the WebCenter application starts.</p> <p>Invalid entries include: <code>/</code>, <code>/foldername/</code>, <code>/foldername/subfolder</code></p> |
| Application Name        | <p>Enter a unique name for this WebCenter Spaces application within this content repository.</p> <p>For example: <code>MyWCS</code></p> <p>The name must begin with an alphabetical character, followed by any combination of alphanumeric characters or the underscore character. The string must be less than or equal to 30 characters.</p>  |

7. Enter connection details for the content repository. For detailed parameter information, see:
- [Table 10–4, "Oracle Content Server Connection Parameters"](#)
  - [Table 10–5, "Oracle Portal Connection Parameters"](#)
  - [Table 10–6, "File System Connection Parameters"](#)

**Table 10–4 Oracle Content Server Connection Parameters**

| Field                 | Description  |
|-----------------------|--|
| CIS Type              | <p>Specify whether Oracle Content Server connects on the content server listener port or the Web server filter, and whether the listener port is SSL enabled. Choose from:</p> <ul style="list-style-type: none"> <li>■ <b>Socket</b> - Uses an <code>intradoc</code> socket connection to connect to the Oracle Content Server. The client IP address must be added to the list of authorized addresses in the Oracle Content Server. In this case, the client is the machine on which Oracle WebCenter is running.</li> <li>■ <b>Socket SSL</b> - Uses an <code>intradoc</code> socket connection to connect to the Oracle Content Server that is secured using the SSL protocol. The client's certificates must be imported in the server's trust store for the connection to be allowed. This is the most secure option, and the recommended option whenever identity propagation is required (for example, in WebCenter Spaces).</li> <li>■ <b>Web</b> - Uses an HTTP(S) connection to connect to the Oracle Content Server.</li> </ul> <p>For WebCenter Spaces, the <b>Web</b> option is not suitable for a back-end Oracle Content Server repository that is being used to store group space and personal space documents, because it does not allow identity propagation.</p> <p>For more information on the configuration parameters required for each CIS socket type, see the table "Oracle Content Server Connection Parameters for Each CIS Socket Type" in <i>Oracle Fusion Middleware Developer's Guide for Oracle WebCenter</i>.</p> |
| Authentication Method | <p>Choose from:</p> <ul style="list-style-type: none"> <li>■ <b>Identity Propagation</b> - Oracle Content Server and the WebCenter application use the same identity store to authenticate users.</li> </ul> <p>(WebCenter Spaces) Identity propagation is required on the active connection for WebCenter Spaces, that is, for the content repository being used to store group space and personal space documents.</p> <ul style="list-style-type: none"> <li>■ <b>External Application</b> - An external application authenticates users against the Oracle Content Server. Select this option if you want to use public, shared, or mapped credentials.</li> </ul> <p>If an external application is used for authentication, use the <b>Associated External Application</b> drop down list to identify the application. If the application you want is not listed, select <b>Create New</b> to define the external application now.</p>  |
| Server Host           | <p>Enter the hostname of the machine where the Oracle Content Server is running.</p> <p>For example: <code>mycontentserver.mycompany.com</code></p> <p>Server Host is required when the CIS Type is set to Socket or Socket SSL.</p>   |

**Table 10–4 (Cont.) Oracle Content Server Connection Parameters**

| <b>Field</b>         | <b>Description</b>  |
|----------------------|---|
| Server Port          | <p>Enter the port on which the Oracle Content Server listens:</p> <ul style="list-style-type: none"> <li>■ Socket - Port specified for the incoming provider in the server.</li> <li>■ Socket SSL - Port specified for the sslincoming provider in the server.</li> </ul> <p>For example, 4444</p> <p>Server Port is required when the CIS Type is set to Socket or Socket SSL.</p>                 |
| Web URL              | <p>Enter the Web server URL for the Oracle Content Server.</p> <p>Use the format: <code>http://&lt;hostname&gt;:&lt;port&gt;/&lt;web_root&gt;/&lt;plugin_root&gt;</code></p> <p>For example: <code>http://mycontentserver/cms/idcplg</code></p> <p>Web URL is applicable when the CIS Type is set to Web.</p>   |
| Key Store Location   | <p>Specify the location of key store that contains the private key used to sign the security assertions. The key store location must be an absolute path.</p> <p>For example: <code>D:\keys\keystore.xyz</code></p> <p>Key Store Location is required when the CIS Type is set to Socket SSL.</p>   |
| Key Store Password   | <p>Enter the password required to access the keystore.</p> <p>For example: <code>T0PS3CR3T</code></p> <p>Key Store Password is required when the CIS Type is set to Socket SSL.</p>   |
| Private Key Alias    | <p>Enter the client private key alias in the keystore. The key is used to sign messages to the server. The public key corresponding to this private key must be imported in the server keystore.</p> <p>Ensure that the alias does not contain special characters or white space. For example: <code>enigma</code></p> <p>Private Key Alias is required when the CIS Type is set to Socket SSL.</p> |
| Private Key Password | <p>Enter the password to be used with the private key alias in the key store.</p> <p>For example: <code>c0d3bR3ak3R</code></p> <p>Private Key Password is required when the CIS Type is set to Socket SSL.</p>  |

**Table 10–5 Oracle Portal Connection Parameters**

| <b>Field</b>     | <b>Description</b>   |
|------------------|--|
| Data Source Name | <p>Enter the JNDI DataSource location used to connect to the portal.</p> <p>For example: <code>jdbc/MyPortalDS</code></p> <p>The datasource must be on the server where the WebCenter application is deployed.</p> |

**Table 10–5 (Cont.) Oracle Portal Connection Parameters**

| Field                           | Description   |
|---------------------------------|---|
| Authentication Method           | <p>Specify how to authenticate users against Oracle Portal. Choose from:</p> <ul style="list-style-type: none"> <li>■ <b>Identity Propagation</b> - Select this option when the WebCenter application and Oracle Portal both use the same user identity store.</li> <li>■ <b>External Application</b> - Use an external application to authenticate users against Oracle Portal. Select this option if you want to use public, shared, or mapped credentials.</li> </ul> <p>If an external application is used for authentication, use the <b>Associated External Application</b> drop-down list to identify the application.</p> |
| Associated External Application | <p>Associate Oracle Portal with an external application. External application credential information is used to authenticate Oracle Portal users.</p> <p>You can select an existing external application from the drop-down list, or click <b>Create New</b> to configure a new external application now.</p>   |

**Table 10–6 File System Connection Parameters**

| Field     | Description  |
|-----------|--|
| Base Path | <p>Enter the full path to a folder on a local file system in which your content is placed. For example: C:\MyContent</p> <p><b>Caution:</b> File system content <i>must not</i> be used in production or enterprise application deployments. This feature is provided for development purposes only.</p> |

8. Click **OK** to save this connection.
9. To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed.

The registered connections are now available to Documents service task flows, which you can add to pages in WebCenter Spaces or custom WebCenter applications. See also, "Working with the Documents Service" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

### 10.3.2 Registering Content Repositories Using WLST

Use the following WLST commands to register new content repository connections:

- **Oracle Content Server** - `createJCRContentServerConnection`
- **File System** - `createJCRFileSystemConnection`
- **Oracle Portal** - `createJCRPortalConnection`

For command syntax and examples, see the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

To configure a particular connection as the default connection, set `isPrimary='true'`. See also, [Section 10.4, "Changing the Active \(or Default\) Content Repository Connection"](#).

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands"](#).

---

---

**Note:** To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed. See "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

---

---

## 10.4 Changing the Active (or Default) Content Repository Connection

WebCenter applications support multiple content repository connections but only one content repository connection can be designated the active (or default) connection.

In WebCenter Spaces, the *active connection* becomes the default back-end repository for group space and personal space documents and the repository must be an Oracle Content Server.

For other WebCenter applications, the *active connection* becomes the default connection for Documents service task flows (Documents, Document List Viewer, Recent Documents). When no specific connection details are provided for these task flows, the default (active) connection is used.

This section contains the following subsections:

- [Changing the Active \(or Default\) Content Repository Connection Using Fusion Middleware Control](#)
- [Changing the Active \(or Default\) Content Repository Connection Using WLST](#)

### 10.4.1 Changing the Active (or Default) Content Repository Connection Using Fusion Middleware Control

To change the active (or default) content repository connection:

1. Log in to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application:
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)
  - [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#)
2. Do one of the following:
  - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings > Service Configuration**.
  - For custom WebCenter applications - From the **Application Deployment** menu, choose **WebCenter > Service Configuration**.
3. From the list of services on the WebCenter Services Configuration page, select **Content Repository**.

The Manage Content Repository Connections table indicates the current active connection (if any).

4. Select the connection you want to become the active (or default) connection, and then click **Edit**.
5. Select the **Active Connection** check box.
6. Click **OK** to update the connection.
7. To start using the updated active connection you must restart the managed server on which the WebCenter application is deployed.

## 10.4.2 Changing the Active (or Default) Content Repository Connection Using WLST

Use the following WLST commands with `Primary='true'` to designate an existing content repository connection as the default connection:

- **Oracle Content Server** - `setJCRContentServerConnection`
- **File System** - `setJCRFileSystemConnection`
- **Oracle Portal** - `setJCRPortalConnection`

For command syntax and examples, see the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

To subsequently disable a default content repository connection, run the same WLST command with `isPrimary='false'`. Connection details are retained but the connection is no longer named as the primary connection in `adf-config.xml`.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands"](#).

---

**Note:** To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed. See, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

---

## 10.5 Modifying Content Repository Connection Details

This section contains the following subsections:

- [Modifying Content Repository Connection Details Using Fusion Middleware Control](#)
- [Modifying Content Repository Connection Details Using WLST](#)

### 10.5.1 Modifying Content Repository Connection Details Using Fusion Middleware Control

To update content repository connection details:

1. Log in to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application:
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)
  - [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#)
2. Do one of the following:
  - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings > Service Configuration**.
  - For custom WebCenter applications - From the **Application Deployment** menu, choose **WebCenter > Service Configuration**.
3. From the list of services on the WebCenter Services Configuration page, choose **Content Repository**.
4. Select the connection name, and click **Edit**.
5. Edit connection details, as required. For detailed parameter information, see:

- [Table 10–4, "Oracle Content Server Connection Parameters"](#)
  - [Table 10–5, "Oracle Portal Connection Parameters"](#)
  - [Table 10–6, "File System Connection Parameters"](#)
6. Click **OK** to save your changes.
  7. To start using the updated (active) connection details, you must restart the managed server on which the WebCenter application is deployed.

## 10.5.2 Modifying Content Repository Connection Details Using WLST

Use the following WLST commands to edit content repository connections:

- **Oracle Content Server** - `setJCRContentServerConnection`
- **File System** - `setJCRFileSystemConnection`
- **Oracle Portal** - `setJCRPortalConnection`

For command syntax and examples, see the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

To configure a particular connection as the active (or default) connection, set `isPrimary='true'`. See also, [Section 10.4, "Changing the Active \(or Default\) Content Repository Connection"](#).

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands"](#).

---

---

**Note:** To start using the updated (active) connection details, you must restart the managed server on which the WebCenter application is deployed. See, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

---

---

## 10.6 Deleting Content Repository Connections

This section contains the following subsections:

- [Deleting Content Repository Connections Using Fusion Middleware Control](#)
- [Deleting Content Repository Connections Using WLST](#)

---

---

**Caution:** Delete a content repository connection only if it is not in use. If a connection is marked as active, it should first be removed from the active list, and then deleted.

---

---

### 10.6.1 Deleting Content Repository Connections Using Fusion Middleware Control

To delete a content repository connection:

1. Log in to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application:
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)
  - [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#)



2. Do one of the following:
  - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings > Service Configuration**.
  - For custom WebCenter applications - From the **Application Deployment** menu, choose **WebCenter > Service Configuration**.
3. From the list of services on the WebCenter Services Configuration page, choose **Content Repository**.
4. Select the connection name, and click **Delete**.
5. To effect this change you must restart the managed server on which the WebCenter application is deployed.

## 10.6.2 Deleting Content Repository Connections Using WLST

Use the WLST command `deleteConnection` to remove a content repository connection. For command syntax and examples, see "deleteConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands"](#).

---

---

**Note:** To effect this change you must restart the managed server on which the WebCenter application is deployed. See, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

---

---

## 10.7 Setting Connection Properties for the WebCenter Spaces Content Repository

You can view, modify, and delete connection properties for the back-end Oracle Content Server repository that is being used by WebCenter Spaces to store group space and personal space documents. Specifically, you can define the root folder under which group space content is stored, the name of the content repository administrator, and a unique application identifier for separating application data on the Oracle Content Server.

This section contains the following subsections:

- [Setting Connection Properties for the WebCenter Spaces Content Repository Using Fusion Middleware Control](#)
- [Setting Connection Properties for the WebCenter Spaces Content Repository Using WLST](#)

### 10.7.1 Setting Connection Properties for the WebCenter Spaces Content Repository Using Fusion Middleware Control

To set content repository connection properties:

1. Log in to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application. See [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#).
2. From the **WebCenter** menu, choose **Settings > Service Configuration**.

3. From the list of services on the WebCenter Services Configuration page, choose **Content Repository**.
4. Select the connection name, and click **Edit**.
5. (For the active connection in WebCenter Spaces only.) Set connection properties for the WebCenter Spaces repository (see [Table 10-7](#)).

**Table 10-7 Content Repository Connection - WebCenter Spaces Repository Details**

| Field                   | Description   |
|-------------------------|---|
| Administrator User Name | Enter the user name of the content repository administrator.<br>For example: <code>sysadmin</code><br>Administrative privileges are required for this connection so that operations can be performed on behalf of WebCenter users.  |
| Spaces Root             | Enter the root folder under which group space content is stored. Specify a folder that does not yet exist and is unique across applications. Use the format: <code>/foldername</code> . This name cannot be the same as the Application Name.<br>For example: <code>/MyWebCenterSpaces</code><br>If it does not already exist, the folder specified is automatically created when the WebCenter application starts.<br>Invalid entries include: <code>/</code> , <code>/foldername/</code> , <code>/foldername/subfolder</code> |
| Application Name        | Enter a unique name for this WebCenter Spaces application within this content repository.<br>For example: <code>MyWCS</code><br>The name must begin with an alphabetical character, followed by any combination of alphanumeric characters or the underscore character. The string must be less than or equal to 30 characters.   |

6. Click **OK** to save your changes.
7. To start using the updated (active) connection properties, you must restart the managed server on which the WebCenter application is deployed.

## 10.7.2 Setting Connection Properties for the WebCenter Spaces Content Repository Using WLST

The following commands are valid only for the WebCenter Spaces application to view, set, and delete properties for the Oracle Content Server repository that is being used by WebCenter Spaces to store group space and personal space documents:

- `listDocumentsSpacesProperties`
- `setDocumentsSpacesProperties`
- `deleteDocumentsSpacesProperties`

For command syntax and detailed examples, see the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands"](#).

## 10.8 Testing Content Repository Connections

After setting up content repository connections, you can test them to make sure that you can access the content repository:

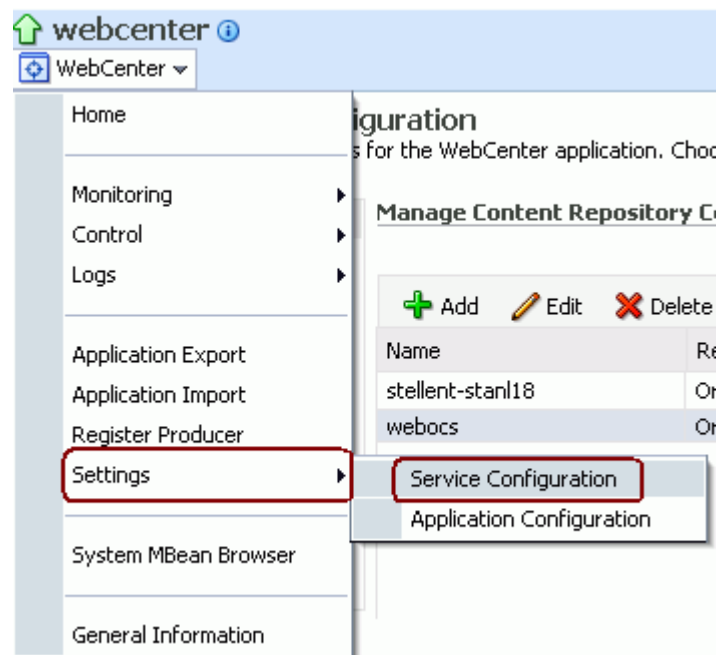
- [Testing Oracle Content Server Connections](#)
- [Testing Oracle Portal Connections](#)

### 10.8.1 Testing Oracle Content Server Connections

To verify a connection of the socket type web, log in to the Web interface of Oracle Content Server as administrator. You can obtain the URL of a socket type connection through Fusion Middleware Control as follows:

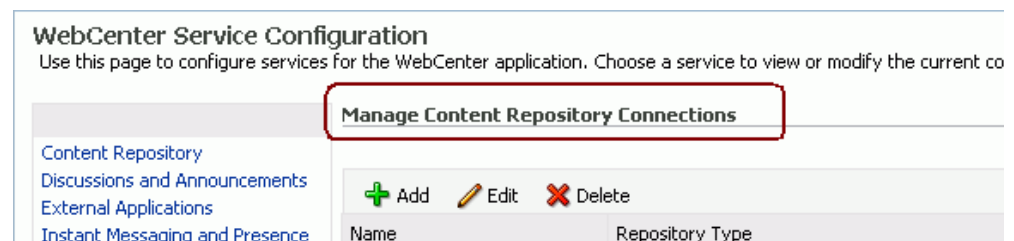
1. In Fusion Middleware Control, from the **WebCenter** menu, choose **Settings** and select **Service Configuration** (Figure 10-4).

**Figure 10-4** Fusion Middleware Control WebCenter Menu



2. On the **Manage Content Repository Connections** page, select the connection and click **Edit** (Figure 10-5).

**Figure 10-5** Manage Content Repository Connections Page

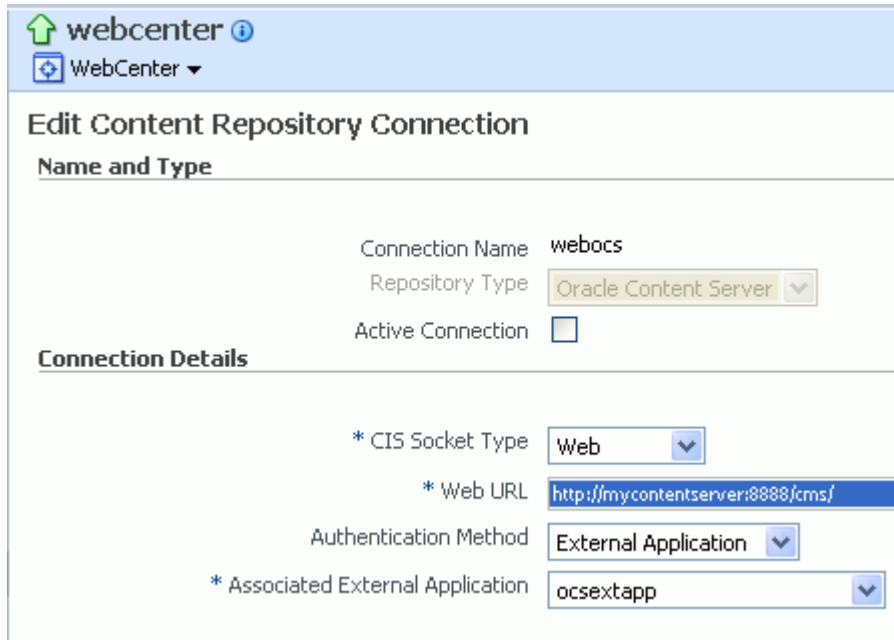


3. On the **Edit Content Repository Connection** page, copy the Web URL (Figure 10-6).

**Note:** Remove the /idcplg/ suffix from the URL before using it.

The URL format is: `http://host_name/web_root/`  
 For example: `http://mycontentserver/cms/`

**Figure 10–6 Edit Content Repository Connection Page**



## 10.8.2 Testing Oracle Portal Connections

To verify the full state of an Oracle Portal connection:

1. In the Oracle WebLogic Administration Console, under **Domain Structure**, expand **Services** > **JDBC**, then double-click **Data Sources** (Figure 10–7).

**Figure 10–7 Oracle WebLogic Administration Console**



2. On the **Summary of JDBC Data Sources** page, select the data source you intend to test (Figure 10–8).

**Figure 10–8 Summary of JDBC Data Sources Page**

### Summary of JDBC Data Sources

A JDBC data source is an object bound to the JNDI tree that provide can look up a data source on the JNDI tree and then borrow a datab

This page summarizes the JDBC data source objects that have been

[Customize this table](#)

**Data Sources(Filtered - More Columns Exist)**

New Delete

| <input type="checkbox"/> | Name     | JNDI Name     |
|--------------------------|----------|---------------|
| <input type="checkbox"/> | PortalDS | jdbc/PortalDS |

New Delete

3. In the **Settings for *datasource\_name*** section, select the tabs **Monitoring**, then **Testing**. Select the data source target server, then click **Test Data Source** to test the connection (Figure 10–9).

**Figure 10–9 Data Source Settings Section**

**Messages**

✔ Test of PortalDS on server AdminServer was successful.

**Settings for PortalDS**

Configuration Targets Monitoring Control Security Notes

Statistics Testing

Use this page to test database connections in this JDBC data source.

[Customize this table](#)

**Test Data Source(Filtered - More Columns Exist)**

Test Data Source Showing 1

|                          | Server | State |
|--------------------------|--------|-------|
| <input type="checkbox"/> |        |       |

## 10.9 Changing the Maximum File Upload Size

By default, the maximum upload size for files is:

- 2 MB for custom WebCenter applications. This default is imposed by Apache MyFaces Trinidad, which handles uploading files from a browser to the application server.
- 2 GB for WebCenter Spaces applications.

The WebCenter application developer can customize the default file upload size at design time by setting the `UPLOAD_MAX_MEMORY`, `UPLOAD_MAX_DISK_SPACE`, and `UPLOAD_TEMP_DIR` parameters in the `web.xml` file. For information about manually editing `web.xml`, see [Section A.1.2, "web.xml"](#).

For more information, see "Uploading Files to Content Repositories" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

---

---

## Managing Services

This chapter describes how to configure and manage back-end services for WebCenter Spaces and custom WebCenter applications deployed on Oracle WebLogic Server.

Always use Fusion Middleware Control or WLST command-line tool to review and configure back-end services for WebCenter applications. Any changes that you make to WebCenter applications, post deployment, are stored in MDS metadata store as customizations. See [Section 1.3.4, "Oracle WebCenter Configuration Considerations."](#)

---

---

**Note:** Changes that you make to WebCenter services configuration, through Fusion Middleware Control or using WLST, are not dynamic so you will need to restart the managed server on which the WebCenter application is deployed for your changes to take effect. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."](#)

---

---

This chapter includes the following sections:

- [Setting Up Connections for the Discussions and Announcements Services](#)
- [Setting Up Connections for the Instant Messaging and Presence Service](#)
- [Setting Up Connections for the Mail Service](#)
- [Setting Up Connections for the Search Service](#)
- [Setting Up Connections for the Worklist Service](#)
- [Setting Up the WebCenter Repository](#)
- [Setting Up the MDS Repository](#)
- [Setting Up the Server for Wiki and Blog Services](#)
- [Setting Up the RSS Service](#)

### Audience

The content of this chapter is intended for Fusion Middleware administrators (users granted the `Admin` or `Operator` role through the Oracle WebLogic Server Administration Console). See also, [Section 1.8, "Understanding Administrative Operations, Roles, and Tools"](#).

## 11.1 Setting Up Connections for the Discussions and Announcements Services

This section contains the following subsections:

- [What You Should Know About Discussion Server Connections](#)
- [Discussion Server Prerequisites](#)
- [Registering Discussion Servers](#)
- [Choosing the Active Connection for Discussions and Announcements](#)
- [Modifying Discussion Server Connection Details](#)
- [Deleting Discussion Server Connections](#)
- [Setting Up Discussions Service Defaults](#)
- [Setting Up Announcements Service Defaults](#)
- [Testing Discussion Server Connections](#)

### 11.1.1 What You Should Know About Discussion Server Connections

The Discussions service enables users to start, publish, and store discussions and announcements in WebCenter applications. The Announcements service lets you create and expose announcements on your application pages.

Both the Discussions service and the Announcements service require a discussion server. The Oracle WebCenter Discussions software is available on the companion CD provided with Oracle Fusion Middleware. For information on installation, see *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*.

The Discussions service and the Announcements service then require a connection to the discussion server. Both services use the same connection. You can register discussion server connections for your WebCenter application through the Fusion Middleware Control Console or using WLST:

- [Registering Discussion Servers Using Fusion Middleware Control](#)
- [Registering Discussion Servers Using WLST](#)

#### WebCenter Spaces

Some additional configuration is required to use Discussions and Announcements services in WebCenter Spaces. This includes choosing the category (on the discussion server) under which all WebCenter Spaces discussions and announcements are stored, and more. This configuration takes place inside WebCenter Spaces. For more detail, see [Section 18.8, "Setting Discussion Forum Options"](#).

In WebCenter Spaces, the `group.mapping` parameter determines whether a subcategory or a single forum is created on the discussion server for new group spaces. For more detail, see [Table 11-4, "Additional Discussion Connection Properties"](#).

You can register additional discussion server connections through the Fusion Middleware Control Console, but only one connection is active at a time.

### 11.1.2 Discussion Server Prerequisites

This section contains the following subsections:

- [Discussion Server - Installation](#)



- [Discussion Server - Configuration](#)
- [Discussion Server - Security Considerations](#)
- [Discussion Server - Limitations](#)

#### 11.1.2.1 Discussion Server - Installation

The Oracle WebCenter Discussions software is available on the companion CD provided with Oracle Fusion Middleware. For information on installation, see *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*.

#### 11.1.2.2 Discussion Server - Configuration

Oracle recommends using same Oracle Internet Directory (OID)-LDAP server for identity management in the discussion server and the WebCenter application. If you are not using OID-LDAP for identity management across the discussion server and the WebCenter application that uses the Discussions service, then users must be configured in the discussion server using the admin user interface at `http://<host>:<port>/owc_discussions/admin`. For more information, see the Jive Forums documentation on the WebCenter product page in the Fusion Middleware documentation library.

For information on reassociating the identity store, see [Section 14.3, "Configuring the Identity Store."](#)

#### 11.1.2.3 Discussion Server - Security Considerations

By default, the Oracle WebCenter Discussions allows unsecured Web service calls. You can optionally configure Oracle WebCenter Discussions to enable the Web Services Security (WS-Security) trusted authentication. WS-Security establishes a trust relationship between your WebCenter application and Oracle WebCenter Discussions so that your WebCenter application can pass the user identity information to the server without knowing the user's credentials.

To enable the WS-Security trusted authentication for Oracle WebCenter Discussions, you must:

- Obtain a valid client and server certificate.
- Configure WS-Security-related properties on the system that hosts Oracle WebCenter Discussions.
- Add the WS-Security-related properties in your Oracle WebCenter Discussions connection created for integrating Discussions and Announcements services into your WebCenter applications. See also, [Table 11-4, "Additional Discussion Connection Properties"](#).

To configure WS-Security, on the server side you must edit the keystore certificate and delete the `webservices.soap.permissionHandler.className` system property.

For details, see [Section 14.8.2, "Securing the Discussions Server with WS-Security."](#)

#### 11.1.2.4 Discussion Server - Limitations

Oracle WebCenter Discussions cannot be started or stopped from WebLogic Server Admin Console. To start or stop the discussion server, you must start or stop the WLS\_Services managed server where Oracle WebCenter Discussions is deployed.

After Oracle WebCenter Discussions has been installed from the WebCenter installation, the only user name/password it will accept is `weblogic/weblogic`

(regardless of the name/password you enter during installation). To change the password or to create another system admin user in the discussion server, you first must log on with weblogic/weblogic. For more information, see "Granting Administrator Role to a Non-Default User" in the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*.

The Oracle WebCenter Discussions URL supports only English and Spanish languages for displaying labels; however, data can be entered in UTF-8 format. Oracle recommends to use the WebCenter application (with all WebCenter-supported languages) for user operations in the discussion server. All WebCenter-supported languages are supported for data, such as discussion topics or announcements, and they are displayed in discussion server also.

(WebCenter Spaces) Do not change user permissions in the discussion server, as this might cause unexpected behavior. Always manage user permissions for discussions and announcements in WebCenter Spaces. See also [Section 19.1.4, "Understanding Discussions Server Role and Permission Mapping."](#)

### 11.1.3 Registering Discussion Servers

You can register multiple discussion server connections with a WebCenter application, but only one of them is active at a time.

To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed.

This section contains the following subsections:




- [Registering Discussion Servers Using Fusion Middleware Control](#)
- [Registering Discussion Servers Using WLST](#)

#### 11.1.3.1 Registering Discussion Servers Using Fusion Middleware Control

To register a discussion server connection:

1. Login to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application:
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)
  - [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#)
2. Do one of the following:
  - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings > Service Configuration**.
  - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter > Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, choose **Discussions and Announcements**.
4. To connect to a new discussion server, click **Add** ([Figure 11-1](#)).

**Figure 11–1 Configuring Discussion and Announcement Connections**

| Manage Discussion and Announcement Connections  |  |                   |
|---|--|-------------------|
|  Add  Edit  Delete |  |                   |
| Name  | Server URL                             | Active Connection |
| Jive-Stahx12-7005   | http://stahx12.us.oracle.com:7005/owc_ |                   |

5. Enter a unique name for this connection, and indicate whether this connection is the active (or default) connection for the application.

See also, [Table 11–1, "Discussion and Announcement Connection - Name"](#).

**Table 11–1 Discussion and Announcement Connection - Name**

| Field             | Description   |
|-------------------|---|
| Connection Name   | Enter a unique name for the connection.<br>The name must be unique (across all connection types) within the WebCenter application.  |
| Active Connection | Select to use this connection for discussion and announcement services in the WebCenter application.<br>While you can register multiple discussion server connections for a WebCenter application, only one connection is used for discussion and announcement services—the default (or active) connection. |

6. Enter connection details for the discussion server. For details, see [Table 11–2, "Discussion and Announcement Connection - Connection Details"](#).

**Table 11–2 Discussion and Announcement Connection - Connection Details**

| Field                   | Description  |
|-------------------------|--|
| Server URL              | Enter the URL of the discussion server hosting Discussions and Announcements.<br>For example: <code>http://discuss-server.com:8888/owc_discussions</code>  |
| Administrator User Name | Enter the user name of the discussion server administrator.<br>This account is used by the Discussions and Announcement services to perform administrative operations on behalf of WebCenter users.<br>In WebCenter Spaces, this account is mostly used for managing group space discussions and announcements. It is not necessary for this user to be a <code>super admin</code> . However, the user must have administrative privileges on the application root category configured for the WebCenter Spaces, that is, the category (on the discussion server) under which all group space discussions and announcement are stored. |
| Connection Secured      | Indicate whether a secured (WS-Security) discussion server connection should be established.<br>If selected, that is, a secure connection is required, use the <b>Additional Properties</b> section to specify the keystore information. See also, <a href="#">Table 11–4, "Additional Discussion Connection Properties"</a> .   |

7. Configure advanced options for the discussion and announcement connection. For details, see [Table 11-3, "Discussion and Announcement Connection - Advanced Configuration"](#).

**Table 11-3 Discussion and Announcement Connection - Advanced Configuration**

| Field                           | Description  |
|---------------------------------|--|
| Connection Timeout (in Seconds) | Specify a suitable timeout for the connection.<br><br>This is the length of time (in seconds) the WebCenter application waits for a response from the discussion server before issuing a connection timeout message.<br><br>The default is -1 which means that the service default is used. The service default is 10 seconds. |

8. Sometimes, additional parameters are required to connect to the discussion server. For example, those listed in [Table 11-4, "Additional Discussion Connection Properties"](#).

**Table 11-4 Additional Discussion Connection Properties**

| Additional Connection Property       | Description   |
|--------------------------------------|---|
| <code>keystore.location</code>       | Certificate file path in your local directory.<br><br>Keystore information is needed only when the discussion forum connection should communicate with the discussion server over WS-Security. For more information, see <a href="#">Section 11.1.2.3, "Discussion Server - Security Considerations."</a>   |
| <code>keystore.password</code>       | Keystore password.  |
| <code>keystore.type</code>           | Keystore type associated with the certificate. Valid values are: <code>jks</code> (Java Key Store) and <code>pks</code> .   |
| <code>encryption.key.alias</code>    | Key alias to be used for encryption.  |
| <code>encryption.key.password</code> | Password for accessing the encryption key.  |
| <code>group.mapping</code>           | (WebCenter Spaces only) Determines whether a subcategory or a single forum is created on the discussion server for new group spaces. When set to <code>forum</code> (the default), a single forum is created under the application root category per group space. When set to <code>category</code> , a subcategory is created under the application root category per group space. When a subcategory that supports multiple forums is more suitable, set <code>group.mapping</code> to <code>category</code> .<br><br>If a group space template has been configured with forum-based taxonomy, then the template takes precedence over this connection entry. If a group space template does not define the mapping (the Blank template, for example), then this <code>group.mapping</code> property is used. If there is no value in the template or the connection, then the default setting is used (forum). |

If additional parameters are required to connect to the discussion server, expand **Additional Properties** and enter details as required (see [Table 11-5, "Discussion and Announcement Connection - Additional Properties"](#)).

**Table 11–5 Discussion and Announcement Connection - Additional Properties**

| Field  | Description  |
|--------|--|
| Add    | <p>Click <b>Add</b> to specify an additional connection parameter:</p> <ul style="list-style-type: none"> <li>■ <b>Name</b> -Enter the name of the connection property.</li> <li>■ <b>Value</b> - Enter the default value for the property.</li> <li>■ <b>Is Property Secured</b> - Indicate whether encryption is required. When selected, the property value is stored securely using encryption.</li> </ul> <p>For example, select this option to secure the <code>admin.password</code> property where the value is the actual password.</p> |
| Delete | <p>Click <b>Delete</b> to remove a selected property.</p> <p>Select the correct row before clicking <b>Delete</b>.</p> <p>Note: Deleted rows appear disabled until you click <b>OK</b>.</p>  |

9. Click **OK** to save this connection.

10. To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."](#)

For WebCenter Spaces, some additional configuration is recommended for the Discussions service. For details, see [Section 18.8, "Setting Discussion Forum Options."](#)

### 11.1.3.2 Registering Discussion Servers Using WLST

Use the WLST command `createDiscussionForumConnection` to create a discussion server connection. For command syntax and examples, see "createDiscussionForumConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

To configure the Discussions and Announcements services to actively use the new discussion server connection, set `default=true`.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

---

**Note:** To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed. See, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

---

## 11.1.4 Choosing the Active Connection for Discussions and Announcements

You can register multiple discussion server connections with a WebCenter application but only one connection is active at a time.

For WebCenter Spaces and any custom WebCenter applications, the *active connection* becomes the back-end discussion server for:

- Discussions task flows (Discussion Forum Manager, Discussions, Popular Topics, Recent Topics, Watched Forums, Watched Topics)
- Announcements task flows (Announcements Manager, Announcements)

This section contains the following subsections:

- [Choosing the Active Connection for Discussions and Announcements Using Fusion Middleware Control](#)
- [Choosing the Active Discussion for Discussions and Announcements Using WLST](#)

#### 11.1.4.1 Choosing the Active Connection for Discussions and Announcements Using Fusion Middleware Control

To change the active connection:

1. Login to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application:
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)
  - [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#)
2. Do one of the following:
  - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings > Service Configuration**.
  - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter > Service Configuration**.
3. From the list of services on the WebCenter Services Configuration page, choose **Discussions and Announcements**.  
 The Manage Discussion and Announcement Connections table indicates the current active connection (if any).
4. Select the connection you want to make the active (or default) connection, and then click **Edit**.
5. Select the **Active Connection** check box.
6. Click **OK** to update the connection.
7. To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."](#)

#### 11.1.4.2 Choosing the Active Discussion for Discussions and Announcements Using WLST

Use the WLST command `setDiscussionForumConnection` with `default=true` to activate an existing discussion server connection. For command syntax and examples, see "setDiscussionForumConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

To disable a Discussions and Announcements connection, either delete it, make another connection the 'active connection', or use the `removeDiscussionForumServiceProperty` command:

```
removeDiscussionForumServiceProperty('appName='webcenter',
property='selected.connection')
```

Using this command, connection details are retained but the connection is no longer named as an active connection. See also, "removeDiscussionForumServiceProperty".

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

---



---

**Note:** To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed. See, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

---



---

## 11.1.5 Modifying Discussion Server Connection Details

You can modify discussion server connection details at any time.

To start using the modified (active) connection you must restart the managed server on which the WebCenter application is deployed.

This section contains the following subsections:

- [Modifying Discussion Server Connection Details Using Fusion Middleware Control](#)
- [Modifying Discussion Server Connection Details Using WLST](#)

### 11.1.5.1 Modifying Discussion Server Connection Details Using Fusion Middleware Control

To update discussion server connection details:

1. Login to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application:
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)
  - [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#)
2. Do one of the following:
  - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings > Service Configuration**.
  - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter > Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, choose **Discussions and Announcements**.
4. Select the connection name, and click **Edit**.
5. Edit connection details, as required. For detailed parameter information, see [Table 11-2, "Discussion and Announcement Connection - Connection Details"](#) and [Table 11-4, "Additional Discussion Connection Properties"](#).
6. Click **OK** to save your changes.
7. To start using the updated (active) connection you must restart the managed server on which the WebCenter application is deployed. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments"](#).

### 11.1.5.2 Modifying Discussion Server Connection Details Using WLST

Use the WLST command `setDiscussionForumConnection` to edit discussion server connection details. For command syntax and examples, see "setDiscussionForumConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.



If additional parameters are required to connect to your discussion server, use the `setDiscussionForumConnectionProperty` command. For details, see "setDiscussionForumConnectionProperty".

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

---

---

**Note:** To start using the updated (active) connection you must restart the managed server on which the WebCenter application is deployed. See, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

---

---

## 11.1.6 Deleting Discussion Server Connections

You can delete discussion server connections at any time but take care when deleting the active connection. If you delete the active connection, none of the Discussions or Announcements task flows will work as they all require a back-end discussion server.

This section contains the following subsections:

- [Deleting a Discussion Server Connection Using Fusion Middleware Control](#)
- [Deleting a Discussion Server Connection Using WLST](#)

### 11.1.6.1 Deleting a Discussion Server Connection Using Fusion Middleware Control

To delete a discussion server connection:

1. Login to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application:
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)
  - [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#)
2. Do one of the following:
  - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings > Service Configuration**.
  - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter > Service Configuration**.
3. From the list of services on the WebCenter Services Configuration page, choose **Discussions and Announcements**.
4. Select the connection name, and click **Delete**.
5. To effect this change you must restart the managed server on which the WebCenter application is deployed. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."](#)

---

---

**Note:** Before restarting the managed server, mark another connection as active; otherwise, the service will be disabled.

---

---



### 11.1.6.2 Deleting a Discussion Server Connection Using WLST

Use the WLST command `deleteConnection` to remove a discussion server connection. For command syntax and examples, see "deleteConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

Ensure that another connection is marked active; otherwise, the service will be disabled.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

---



---

**Note:** To effect this change you must restart the managed server on which the WebCenter application is deployed. See, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

---



---

### 11.1.7 Setting Up Discussions Service Defaults

Use the WLST command `setDiscussionForumServiceProperty` to set defaults for the Discussions service:

- `topics.fetch.size`: Maximum number of topics fetched by the Discussions service and displayed in the topics view.
- `forums.fetch.size`: Maximum number of forums fetched by the Discussions service and displayed in the forums view.
- `recentTopics.fetch.size`: Maximum number of topics fetched by the Discussions service and displayed in the recent topics view.
- `watchedTopics.fetch.size`: Maximum number of topics fetched by the Discussions service and displayed in the watched topics view.
- `watchedForums.fetch.size`: Maximum number of forums fetched by the Discussions service and displayed in the watched forums view.
- `application.root.category.id`: Application root category ID on the discussion server under which all discussion forums are stored. For example, if set to 3, all forums are stored inside category 3.
- `ForumGatewayManager.AUTO_START`: Mail communication through group space mail distribution lists of a mail server can be published as discussion forum posts on a discussion server, as described in [Section 18.8.3, "Enabling Discussion Forums to Publish Group Space Mail."](#) This parameter starts or stops the gateway for this communication.

For WebCenter Spaces, the default value is true, which means that as soon as you configure mail server settings through WebCenter Spaces administration, the gateway will start. Set this to false, and restart the managed server, to stop the gateway and disable this feature.

For custom WebCenter applications, the default value is false. Set this to true, and restart the managed server, to start the gateway and enable this feature.

For command syntax and examples, see "setDiscussionForumServiceProperty" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

### 11.1.8 Setting Up Announcements Service Defaults

Use the WLST command `setAnnouncementServiceProperty` to set defaults for the Announcements service:

- `miniview.page_size`: Maximum number of announcements displayed in the Announcements sidebar view.
- `mainview.page_size`: Maximum number of announcements displayed in the Announcements main view.
- `linksview.page_size`: Maximum number of announcements displayed in the Announcements links view.
- `announcements.expiration.days`: Number of days that announcements display and remain editable.

For command syntax and examples, see "setAnnouncementServiceProperty" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

### 11.1.9 Testing Discussion Server Connections

Try accessing the discussion server with the following URL:

`http://host:port/owc_discussions`. You should see a page listing all public information.

## 11.2 Setting Up Connections for the Instant Messaging and Presence Service

This section contains the following subsections:

- [What You Should Know About Instant Messaging and Presence Connections](#)
- [Instant Messaging and Presence Server Prerequisites](#)
- [Registering Instant Messaging and Presence Servers](#)
- [Choosing the Active Connection for Instant Messaging and Presence](#)
- [Modifying Instant Messaging and Presence Connection Details](#)
- [Deleting Instant Messaging and Presence Connections](#)
- [Setting Up Instant Messaging and Presence Service Defaults](#)
- [Testing Instant Messaging and Presence Connections](#)

### 11.2.1 What You Should Know About Instant Messaging and Presence Connections

The Instant Messaging and Presence (IMP) service enables you to observe the presence status of other authenticated application users (online, offline, busy, or idle) and provides instant access to interaction options, such as phone calls, instant messages (IM), and mails. Users can also receive notifications from configured voicemail systems. A single connection to a back-end presence server is required.

A presence server, Oracle WebLogic Communications (OWLCS), is bundled with Oracle Fusion Middleware, but WebCenter is certified with Microsoft Live Communications Server (LCS) and can integrate with other presence servers. For

information on installation, see *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*.

---

---

**Note:** To add or remove buddies to your account, you must use the OWLCS/LCS client. In WebCenter applications you can see buddies but you cannot add or remove buddies. For more information, see *Oracle WebLogic Communication Services Administrator's Guide*.

---

---

You can register presence server connection for your WebCenter application through the Fusion Middleware Control Console or using WLST:

- [Registering Instant Messaging and Presence Servers Using Fusion Middleware Control](#)
- [Registering Instant Messaging and Presence Servers Using WLST](#)

You must mark a connection as active for the service to work. You can register additional presence server connections, but only one connection is active at a time.

## 11.2.2 Instant Messaging and Presence Server Prerequisites

This section contains the following subsections:

- [Oracle WebLogic Communications Server \(OWLCS\) Prerequisites](#)
- [Microsoft Live Communications Server \(LCS\) Prerequisites](#)

### 11.2.2.1 Oracle WebLogic Communications Server (OWLCS) Prerequisites

For OWLCS prerequisites, see the *Oracle WebLogic Communication Services Installation Guide*.

#### 11.2.2.1.1 OWLCS - Installation

For detailed OWLCS installation instructions, see the *Oracle WebLogic Communication Services Installation Guide*.

#### 11.2.2.1.2 OWLCS - Configuration

OWLCS supports both identity propagation and external application-based connections. Oracle recommends using identity propagation for OWLCS connections, since additional security can be set with WS-Security.

OWLCS and the WebCenter application should point to the same LDAP-based identity store. If the OWLCS server and the WebCenter application use different LDAP-based identity stores, then you must configure an external application for the connection so that users can supply credentials to authenticate themselves on the OWLCS server.

For information on reassociating the WebCenter applications identity store, see [Section 14.3, "Configuring the Identity Store."](#)

If necessary, reconfigure OWLCS to use the same identity store. For more information, see the *Oracle WebLogic Communication Services Administrator's Guide*.

#### 11.2.2.1.3 OWLCS - Security Considerations

If the OWLCS server is running with WS-Security enabled, then the administrator must set the `policyURI` parameter in the presence server connection.

If WS-Security is not required, then the administrator should disable WS-Security on the OWLCS server.

For details, see [Section 14.8.3, "Securing Oracle WebLogic Communication Services \(OWLCS\) with WS-Security."](#)

See also, [Section 14.6.10, "Securing the WebCenter Spaces Connection to OWLCS with SSL."](#)

#### **11.2.2.1.4 OWLCS - Limitations**

With OWLCS, user creation and deletion is manual. Any time a new user is added to (or removed from) the application's identity store, the same user must be created in (or removed from) the OWLCS user store.

Each OWLCS user has a watcher list, which is a list of the other users allowed to see his presence. This watcher list must be under 125 KB (approximately 400 users). In WebCenter, the presence of all users must be visible, even if they are not buddies of the logged-in user. To get their presence, WebCenter creates a new account on OWLCS with the group space `guid` and adds this new user as a watcher of the visible users. In other words, each member of a group space has an entry of that group space `guid` in his watcher list. A problem can arise when a user is part of many group spaces. Because the watcher list contains entries for each group space, its size can grow greater than 125KB. When that happens, updates to the watcher list are rejected, giving the user a "Subscription Request" popup with that scope `guid`. If this happens, then the user should just cancel the subscription request.

### **11.2.2.2 Microsoft Live Communications Server (LCS) Prerequisites**

#### **11.2.2.2.1 LCS - Installation**

Refer to the Microsoft Live Communications Server 2005 documentation for installation information.

#### **11.2.2.2.2 LCS - Configuration**

To use Microsoft Live Communications Server 2005 as the communication server for the Instant Messaging and Presence service, you must install the Oracle RTC Web service for Microsoft Live Communications Server 2005.

To install the Oracle RTC Web service for Microsoft Live Communications Server 2005:

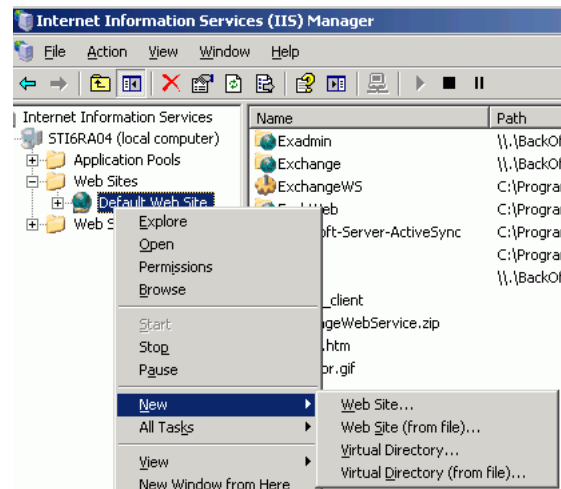
1. Extract the `RTCWebService.zip` file from the Oracle Fusion Middleware companion CD to a folder on the system where Microsoft Live Communications Server 2005 is installed. The zip file contains the following:

```
/Bin  
/images  
ApplicationConfigurationService.asmx  
BlafPlus.css  
ExtAppLogin.aspx  
ExtAppLogin.aspx.cs  
Global.asax  
Log4Net.config
```

RTCService.asmx  
 Web.Config  
 WebcenterTemplate.master

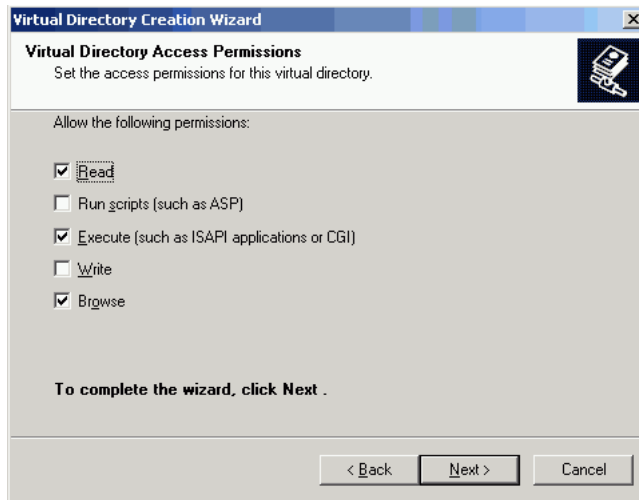
2. Open the Internet Information Services (IIS) Manager.
3. Expand the server node and then **Web Sites** in the Internet Information Services (IIS) Manager window.
4. Right-click **Default Web Site**, select **New**, and then select **Virtual Directory** to create a new site for the Oracle RTC Web service, as shown in [Figure 11–2](#). The Virtual Directory Creation Wizard displays.

**Figure 11–2** *Creating a Virtual Directory*



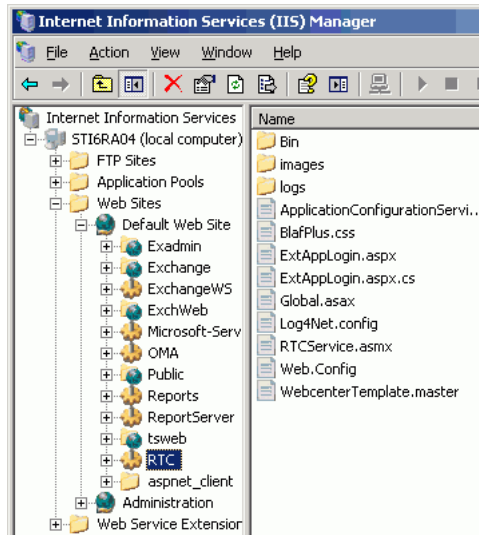
5. Click **Next**.
6. Enter an alias for the virtual directory in the **Alias** field, for example **RTC**.
7. Enter the path to the directory where you extracted the `RTCWebService.zip` file. Alternatively, use the **Browse** button to navigate to that directory.
8. Click **Next**.
9. Ensure that the virtual directory has the Read, Execute, and Browse privileges. ([Figure 11–3](#))

**Figure 11–3 Virtual Directory Properties**

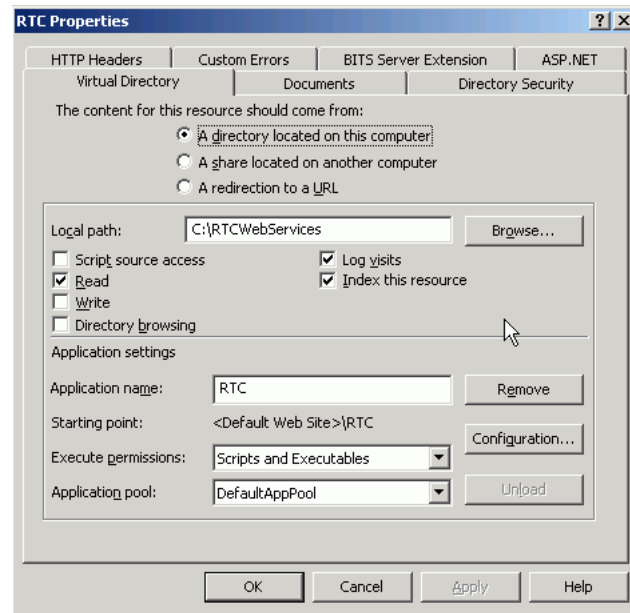


10. Click **Next**.
11. Click **Finish**. The newly created virtual directory appears under **Default Web Site** in the Internet Information Services (IIS) Manager window. (Figure 11–4)

**Figure 11–4 Adding a Virtual Directory**



12. Right-click the newly created virtual directory for the Oracle RTC Web service, and then select **Properties** to open the Properties dialog.
13. In the Virtual Directory tab, under **Application settings**, click **Create**. Notice that the button label changes to **Remove**, and the name of your newly created virtual directory appears in the **Application name** field.
14. Select **Scripts and Executables** from the **Execute permissions** dropdown list, as shown in Figure 11–5.

**Figure 11–5 Virtual Directory Properties**

15. Under the **ASP.NET** tab, select the ASP.NET version as 2.0 or higher from the **ASP.NET version** dropdown list. IIS should be configured to consume ASP.NET 2.0 applications.
16. Click **OK**.
17. Ensure that the LSC pool name in the LCS connection has been set.
18. Test the Web service by accessing the Web site from the following URL format:

```
http://localhost/default_
website/ApplicationConfigurationService.asmx
```

Where *default\_website* refers to the virtual directory that you created for the Oracle RTC Web service.

For example:

```
http://localhost/RTC/ApplicationConfigurationService.asmx
```

#### 11.2.2.3 LCS - Security Considerations

You must configure an external application for Microsoft Live Communications Server connections so that users can supply credentials to authenticate themselves on the LCS server.

With a secured application, users get buddies and presence status. With LCS, if security is required, then LCS should be on a private trusted network.

LCS provides an option for changing external credentials, which works as an alternative to using an external application. A logged-in user can click any Presence tag and select **Change Credentials** from the menu.

See also, [Section 11.2.3.1, "Registering Instant Messaging and Presence Servers Using Fusion Middleware Control."](#)

#### 11.2.2.4 LCS - Limitations

WebCenter applications do not support phone conferencing.

## 11.2.3 Registering Instant Messaging and Presence Servers

You can register multiple presence server connections with a WebCenter application but only one of them is active at a time.

To start using the new (active) presence server you must restart the managed server on which the WebCenter application is deployed.

This section contains the following subsections:

- [Registering Instant Messaging and Presence Servers Using Fusion Middleware Control](#)
- [Registering Instant Messaging and Presence Servers Using WLST](#)


### 11.2.3.1 Registering Instant Messaging and Presence Servers Using Fusion Middleware Control

To register a presence server connection:

1. Login to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application:
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)
  - [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#)
2. Do one of the following:
  - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings > Service Configuration**.
  - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter > Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, choose **Instant Messaging and Presence**.
4. To connect to a new presence server, click **Add** ([Figure 11-6](#)).

**Figure 11-6** *Configuring Instant Messaging and Presence Services*

#### Manage Instant Messaging and Presence Connections

|  Add  Edit  Delete |                 |            |                   |
|---|-----------------|------------|-------------------|
| Name  | Connection Type | Server URL | Active Connection |
| No Data Available   |                 |            |                   |

5. Enter a unique name for this connection, specify the presence server type, and indicate whether this connection is the active (or default) connection for the application.

See also, [Table 11-6, "Instant Messaging and Presence Connection - Name"](#).



**Table 11–6 Instant Messaging and Presence Connection - Name**

| Field             | Description  |
|-------------------|--|
| Name              | Enter a unique name for the connection. The name must be unique (across all connection types) within the WebCenter application.  |
| Connection Type   | Specify the type of presence server you want to connect to: <ul style="list-style-type: none"> <li>■ OWLCS - Oracle WebLogic Communications Server</li> <li>■ LCS - Microsoft's Live Communication Server</li> </ul> Out-of-the-box, two presence connection types are available—OWLCS and LCS.                        |
| Active Connection | Select to use this connection in the WebCenter application for instant messaging and presence services.<br><br>While you can register multiple presence server connections for a WebCenter application, only one connection is used by the Instant Messaging and Presence service— the default (or active) connection. |

6. Enter connection details for the server hosting instant messaging and presence services.

For detailed parameter information, see [Table 11–7, "Instant Messaging and Presence Connection - Connection Details"](#).

**Table 11–7 Instant Messaging and Presence Connection - Connection Details**

| Field                   | Description  |
|-------------------------|--|
| Server URL              | Enter the URL of the sever hosting instant messaging and presence services.<br><br>For example: <code>http://myowlcshost.com:8888</code>   |
| Domain                  | Enter the domain associated with this connection.<br><br>The domain specified is used to construct each user's IM ID. For example, if the domain is <code>oracle.com</code> and presence is requested for user with name <code>john</code> then the IM address resolved will be <code>john@oracle.com</code> .<br><br>If the user IM address needs to be resolved from the OID/LDAP server, then specify the user profile attribute that will provide the IM address here as <code>profile:&lt;attribute&gt;</code> where <code>profile</code> is a keyword and <code>attribute</code> is the user profile attribute name where the IM address is stored. For example, <code>profile:primarySipAddress</code> .<br><br>The IM ID for OWLCS and LCS will be the SIP ID; that is, <code>sip:john@oracle.com</code> . SIP s short for Session Initiation Protocol - an Internet protocol for live communication between people. |
| Administrator User Name | (OWLCS Only) Enter the user name of the presence server administrator.<br><br>Administrative privileges are required for this connection so that operations can be performed on behalf of WebCenter users.   |
| Administrator Password  | (OWLCS Only)Enter the password for the administrator.  |

**Table 11–7 (Cont.) Instant Messaging and Presence Connection - Connection Details**

| Field                           | Description  |
|---------------------------------|--|
| Authentication Method           | <p>(OWLCS Only) Specify how to authenticate users against the instant messaging and presence server. Choose from:</p> <ul style="list-style-type: none"> <li>▪ <b>Identity Propagation</b> - Select this option if you want the application and OWLCS to use the same user identity.</li> <li>▪ <b>External Application</b> - Use an external application to authenticate users against the instant messaging and presence server. Select this option if you want to use public, shared, or mapped credentials.</li> </ul> <p>If an external application is used for authentication, use the <b>Associated External Application</b> drop down list to identify the application. If the application you want is not listed, select <b>Create New...</b> to define the external application now.</p>                   |
| Associated External Application | <p>Associate the instant messaging and presence server with an external application. External application credential information is used to authenticate users against the instant messaging and presence server.</p> <p>An external application is mandatory for LCS server connections.</p> <p>You can select an existing external application from the drop-down list, or click <b>Create New</b> to configure a new external application.</p> <p>The external application you configure for the Instant Messaging and Presence service must use the <code>POST</code> authentication method, and specify an additional field named <code>Account</code> (Name property) that is configured to <code>Display to User</code> (checked). See also <a href="#">Chapter 13, "Managing External Applications."</a></p> |
| LCS Pool Name                   | <p>(LCS Only) Enter the name of the Microsoft Live Communication Server pool used for this connection. The pool name is mandatory for LCS connections.</p> <p>Refer to <i>Microsoft Live Communication Server</i> documentation for details on the pool name.</p>  |
| Connection Timeout (in seconds) | <p>Specify a suitable timeout for the connection.</p> <p>This is the length of time (in seconds) the WebCenter application waits for a response from the presence server before issuing a connection timeout message.</p> <p>The default is -1 which means that the service default is used. The service default is 10 seconds.</p>  |
| Policy URI                      | <p>(OWLCS Only) URI to the WS-Security policy that is required for authentication on the Oracle WebLogic Communication Server. Specify <code>oracle/wss11_saml_token_with_message_protection_client_policy</code> when OWLCS is WS-Security enabled.</p>   |

7. Sometimes, additional parameters are required to connect to the presence server.

If WS-Security is enabled on this connection, add an additional property named `recipient.alias` and enter the alias used to import the OWLCS certificate. Ensure that this value is unique and is not used already by some other service. If no alias name is supplied, then the default value is used (`webcenter_owlcs`).

[Table 11–8, "Additional IMP Connection Properties"](#) lists additional parameters.

**Table 11–8 Additional IMP Connection Properties**

| <b>Additional Connection Property</b> | <b>Description</b>   |
|---------------------------------------|--|
| <i>presence.url</i>                   | (OWLCS only) URL to the OWLCS Presence service.<br>Required if the OWLCS Presence service is deployed on a separate node. When no value is specified, the <code>Server URL</code> property is used.  |
| <i>contacts.url</i>                   | (OWLCS only) URL to the OWLCS Contact Management service.<br>Required if the OWLCS Contact Management service is deployed on a separate node. When no value is specified, the <code>Server URL</code> property is used.  |
| <i>call.url</i>                       | (OWLCS only) URL to the OWLCS Third Party Call service.<br>Required if the OWLCS Third Party Call service is deployed on a separate node. When no value is specified, the <code>Server URL</code> property is used.  |
| <i>call.method</i>                    | (OWLCS only) Third party call method.<br>Valid values are: <code>sip</code> and <code>pstn</code> . The default value is <code>sip</code> .<br>When set to <code>sip</code> , the IMP service will forward the user's SIP address to the third-party call service. The third-party call service must decide on the routing of the call.<br>If it is set to <code>pstn</code> , then the user's phone number is based on the user's profile attribute ( <code>BUSINESS_PHONE</code> ). This default profile attribute ( <code>BUSINESS_PHONE</code> ) can be changed to any other attribute with the connection property <code>call.number.attribute</code> . |
| <i>call.domain</i>                    | (OWLCS only) Domain name of the PSTN gateway.<br>Required when the <code>call.method</code> is <code>pstn</code> .   |
| <i>contact.number.attribute</i>       | (OWLCS only) User profile attribute used to store users' phone numbers. The default attribute is <code>BUSINESS_PHONE</code> .<br>Required when the <code>call.method</code> is <code>pstn</code> .  |
| <i>primary.domain</i>                 | (OWLCS and LCS) User domain. This property is required when WebCenter user names are qualified with a domain. For example, when user names are <code>xyz@example.com</code> , the <code>primary.domain</code> is <code>example.com</code> .<br>This property is used by <code>IMPAddressResolver</code> to resolve user names to sip-address, and vice-versa. If this property is not supplied, then there could be inconsistencies in the resolver functions, which can affect IMP service performance.   |

If additional parameters are required to connect to the presence server, expand **Additional Properties** and enter details as required (see [Table 11–9, "Instant Messaging and Presence Connection - Additional Properties"](#)).

**Table 11–9 Instant Messaging and Presence Connection - Additional Properties**

| Field  | Description  |
|--------|--|
| Add    | <p>Click <b>Add</b> to specify an additional connection parameter:</p> <ul style="list-style-type: none"> <li>■ <b>Name</b> -Enter the name of the connection property.</li> <li>■ <b>Value</b> - Enter the default value for the property.</li> <li>■ <b>Is Property Secured</b> - Indicate whether encryption is required. When selected, the property value is stored securely using encryption.</li> </ul> <p>For example, select this option to secure the <code>admin.password</code> property where the value is the actual password.</p> |
| Delete | <p>Click <b>Delete</b> to remove a selected property.</p> <p>Select the correct row before clicking <b>Delete</b>.</p> <p>Note: Deleted rows appear disabled until you click <b>OK</b>.</p>  |

8. Click **OK** to save this connection.
9. To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."](#)

### 11.2.3.2 Registering Instant Messaging and Presence Servers Using WLST

Use the WLST command `createIMPConnection` to create a presence server connection. For command syntax and examples, see "createIMPConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

To configure the Instant Messaging and Presence service to actively use a new IMP connection, set `default=true`. See also, [Section 11.2.4.2, "Choosing the Active Connection for Instant Messaging and Presence Using WLST."](#)

---



---

**Note:** To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed. See, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

---



---

## 11.2.4 Choosing the Active Connection for Instant Messaging and Presence

You can register multiple instant messaging and presence server connections with a WebCenter application but only one connection is active at a time.

For WebCenter Spaces and any custom WebCenter application, the *active connection* becomes the back-end presence server for the Buddies task flow.

This section contains the following subsections:

- [Choosing the Active Connection for Instant Messaging and Presence Using Fusion Middleware Control](#)
- [Choosing the Active Connection for Instant Messaging and Presence Using WLST](#)

### 11.2.4.1 Choosing the Active Connection for Instant Messaging and Presence Using Fusion Middleware Control

To change the active connection:

1. Login to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application:
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)
  - [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#)
2. Do one of the following:
  - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings > Service Configuration**.
  - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter > Service Configuration**.
3. From the list of services on the WebCenter Services Configuration page, choose **Instant Messaging and Presence**.  
 The Manage Instant Messaging and Presence Connections table indicates the current active connection (if any).
4. Select the connection you want to make the active (or default) connection, and then click **Edit**.
5. Select the **Active Connection** check box.
6. Click **OK** to update the connection.
7. To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."](#)

### 11.2.4.2 Choosing the Active Connection for Instant Messaging and Presence Using WLST

Use the WLST command `setIMPConnection` with `default=true` to activate an existing presence server connection. For command syntax and examples, see "setIMPConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

To disable a presence server connection, either delete it, make another connection the 'active connection' or use the `removeIMPServiceProperty` command:

```
removeIMPServiceProperty('appName='webcenter', property='selected.connection')
```

Using this command, connection details are retained but the connection is no longer named as an active connection. See also, "removeIMPServiceProperty".

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

---

**Note:** To start using this active connection you must restart the managed server on which the WebCenter application is deployed. See, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

---

## 11.2.5 Modifying Instant Messaging and Presence Connection Details

You can modify instant messaging and presence server connection details at any time.

To start using an updated (active) connection you must restart the managed server on which the WebCenter application is deployed.

This section contains the following subsections:

- [Modifying Instant Messaging and Presence Connections Details Using Fusion Middleware Control](#)
- [Modifying Instant Messaging and Presence Connections Details Using WLST](#)

### 11.2.5.1 Modifying Instant Messaging and Presence Connections Details Using Fusion Middleware Control

To update connection details for an instant messaging and presence server:

1. Login to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application:
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)
  - [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#)
2. Do one of the following:
  - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings > Service Configuration**.
  - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter > Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, choose **Instant Messaging and Presence**.
4. Select the connection name, and click **Edit**.
5. Edit connection details, as required. For detailed parameter information, see [Table 11-7, "Instant Messaging and Presence Connection - Connection Details"](#).
6. Click **OK** to save your changes.
7. To start using the updated (active) connection you must restart the managed server on which the WebCenter application is deployed. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."](#)

### 11.2.5.2 Modifying Instant Messaging and Presence Connections Details Using WLST

Use the WLST command `setIMPConnection` to edit presence server connection details. For command syntax and examples, see "setIMPConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

If additional parameters are required to connect to your presence server, then use the `setIMPConnectionProperty` command. For details, see "setIMPConnectionProperty".

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

---



---

**Note:** To start using the updated (active) connection you must restart the managed server on which the WebCenter application is deployed. See, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

---



---

## 11.2.6 Deleting Instant Messaging and Presence Connections

You can delete instant messaging and presence connections at any time but take care when deleting the active connection. If you delete the active connection, Buddies task flows will not work and user presence options will not be available, as these require a back-end instant messaging and presence server.

When you delete a connection, consider deleting the external application associated with the instant messaging and presence service *if* the application's sole purpose was to support this service. See [Section 13.4, "Deleting External Application Connections."](#)

This section contains the following subsections:

- [Deleting Instant Messaging and Presence Connections Using Fusion Middleware Control](#)
- [Deleting Instant Messaging and Presence Connections Using WLST](#)

### 11.2.6.1 Deleting Instant Messaging and Presence Connections Using Fusion Middleware Control

To delete an instant messaging and presence server connection:

1. Login to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application:
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)
  - [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#)
2. Do one of the following:
  - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings > Service Configuration**.
  - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter > Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, choose **Instant Messaging and Presence**.
4. Select the connection name, and click **Delete**.
5. To effect this change you must restart the managed server on which the WebCenter application is deployed. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."](#)

---



---

**Note:** Before restarting the managed server, mark another connection as active; otherwise, the service will be disabled.

---



---



### 11.2.6.2 Deleting Instant Messaging and Presence Connections Using WLST

Use the WLST command `deleteConnection` to remove a presence server connection. For command syntax and examples, see "deleteConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

## 11.2.7 Setting Up Instant Messaging and Presence Service Defaults

Use the WLST command `setIMPServiceProperty` to set defaults for the IMP service:

- `selected.connection`: Connection used by the Instant Messaging and Presence service.
- `rtc.cache.time`: Cache timeout for instant messaging and presence data.
- `resolve.display.name.from.user.profile`: Information displayed when user names are unavailable.

For command syntax and detailed examples, see "setIMPServiceProperty" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

## 11.2.8 Testing Instant Messaging and Presence Connections

To verify an OWLCS connection, try accessing the endpoint for the following Web services:

- `<protocol>://<host>:<port>/PresenceConsumerService/services/PresenceConsumer`
- `<protocol>://<host>:<port>/PresenceSupplierService/services/PresenceSupplier`
- `<protocol>://<host>:<port>/ThirdPartyCallService/services/ThirdPartyCall`
- `<protocol>://<host>:<port>/services`

To verify an LCS connection, try accessing the endpoint for the WebCenter RTC Web services deployed on it:

- `<protocol>://<host>/RTC/ApplicationConfigurationService.asmx`
- `<protocol>://<host>/RTC/RTCService.asmx`

These Web services expose a set of Web methods that you can invoke to test the validity.

## 11.3 Setting Up Connections for the Mail Service

This section contains the following subsections:

- [What You Should Know About Mail Server Connections](#)
- [Mail Server Prerequisites](#)
- [Registering Mail Servers](#)
- [Choosing the Active \(or Default\) Mail Server Connection](#)



- [Modifying Mail Server Connection Details](#)
- [Deleting Mail Server Connections](#)
- [Setting Up Mail Service Defaults](#)
- [Testing Mail Server Connections](#)

### 11.3.1 What You Should Know About Mail Server Connections

WebCenter supports the Microsoft Exchange Server or any mail server that supports IMAP4 and SMTP. To enable WebCenter users to access mail within a WebCenter application and perform basic operations such as read, reply, and forward, you must first register the appropriate mail server with the WebCenter application. The Mail service is not configured out-of-the-box.

You can register multiple mail server connections:

- **WebCenter Spaces** supports multiple mail connections. The mail connection marked *active* is the default connection for mail services in WebCenter Spaces. All additional connections are offered as alternatives; WebCenter Spaces users can choose which one they want to use through user preferences.
- **Custom WebCenter applications** only use one mail connection—the connection marked *active*. Any additional connections are ignored.

### 11.3.2 Mail Server Prerequisites

This section contains the following subsections:

- [Mail Server - Installation](#)
- [Mail Server - Configuration](#)
- [Mail Server - Security Considerations](#)
- [Mail Server - Limitations](#)

#### 11.3.2.1 Mail Server - Installation

Refer to your mail server documentation for installation information.

#### 11.3.2.2 Mail Server - Configuration

To enable users to access mail services from within a WebCenter application, it is essential that users created on the mail server correspond with the users created in the identity store used by the WebCenter application.

For information about adding users on a mail server, refer to the mail server's product documentation. For more information about adding users to the application's identity store, see [Section 14.3, "Configuring the Identity Store."](#)

For group space distribution lists to work in WebCenter Spaces (or custom WebCenter applications leveraging the WebCenter Spaces group space management feature), WebCenter Spaces must use Microsoft Exchange where distribution lists are managed on an Active Directory server. Group space distribution lists are created automatically whenever a group space is created. To disable this feature with Microsoft Exchange, do not provide the LDAP (Active Directory) server details in the mail connection. See also, step 7 [Section 11.3.3.1, "Registering Mail Servers Using Fusion Middleware Control."](#)

### 11.3.2.3 Mail Server - Security Considerations

See [Section 14.6.8, "Securing the WebCenter Spaces Connection to IMAP and SMTP with SSL."](#)

---

**Note:** If LDAP is configured to run in secure mode, then add the LDAP Secured property (set to true/false) to use LDAP while creating distribution lists. See [Table 11-12](#).

---

### 11.3.2.4 Mail Server - Limitations

In WebCenter Spaces, the Mail service requires a Microsoft Exchange mail server connection to enable automatic group space distribution lists.

## 11.3.3 Registering Mail Servers

You can register multiple mail server connections. To start using the new mail connections you must restart the managed server on which the WebCenter application is deployed.

This section contains the following subsections:

- [Registering Mail Servers Using Fusion Middleware Control](#)
- [Registering Mail Servers Using WLST](#)

### 11.3.3.1 Registering Mail Servers Using Fusion Middleware Control




To register a mail server with WebCenter applications:

1. Login to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application:
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)
  - [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#)
2. Do one of the following:
  - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings > Service Configuration**.
  - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter > Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, choose **Mail Server**.
4. To connect to a new mail server, click **Add** ([Figure 11-7](#)).

**Figure 11-7** *Configuring Mail Servers*

**Manage Mail Server Connections**

---

|  Add  Edit  Delete |                         |                         |                   |
|---|-------------------------|-------------------------|-------------------|
| Name  | IMAP Host               | SMTP Host               | Active Connection |
| MailConnection  | stport13.idc.oracle.com | stport13.idc.oracle.com | ✓                 |

5. Enter a unique name for this connection, and indicate whether this connection is the active (or default) connection for the application.

See also, [Table 11–10, "Mail Server Connection - Name"](#).

**Table 11–10 Mail Server Connection - Name**

| Field             | Description  |
|-------------------|--|
| Name              | Enter a unique name for the connection. The name must be unique (across all connection types) within the WebCenter application.  |
| Active Connection | <p>Select to indicate whether this connection is the default (or active) connection for the Mail service.</p> <p>You can register multiple mail server connections:</p> <ul style="list-style-type: none"> <li>■ <b>WebCenter Spaces</b> supports multiple mail connections. The mail connection marked <i>active</i> is the default connection for mail services in WebCenter Spaces. All additional connections are offered as alternatives; WebCenter Spaces users can choose which one they want to use through user preferences.</li> <li>■ <b>Custom WebCenter applications</b> only use one mail connection—the connection marked <i>active</i>. Any additional connections are ignored.</li> </ul> |

6. Enter connection details for the mail server. For detailed parameter information, see [Table 11–11, "Mail Server Connection Parameters"](#).

**Table 11–11 Mail Server Connection Parameters**

| Field        | Description   |
|--------------|---|
| IMAP Host    | Enter the hostname of the machine where the IMAP (Internet Message Access Protocol) service is running.                                     |
| IMAP Port    | Enter the port on which the IMAP service listens.   |
| IMAP Secured | Indicate whether a secured connection (SSL) is required for incoming mail over IMAP. Valid values are true and false. The default is false. |
| SMTP Host    | Enter the hostname of the machine where the SMTP (Simple Mail Transfer Protocol) service is running.  |
| SMTP Port    | Enter the port on which the SMTP service listens.   |
| SMTP Secured | Indicate whether a secured connection (SSL) is required for outgoing mail over SMTP. Valid values are true and false. The default is false. |

**Table 11–11 (Cont.) Mail Server Connection Parameters**

| Field                           | Description   |
|---------------------------------|---|
| Associated External Application | <p>(Mandatory) Associate the mail server with an external application. External application credential information is used to authenticate users against the IMAP and SMTP servers. The Mail service will use the same credentials to authenticate the user on both IMAP and SMTP.</p> <p>You can select an existing external application from the drop-down list, or click <b>Create New</b> to configure a new external application.</p> <p>The external application you configure for the Mail service must use the <code>POST</code> authentication method, and specify an additional field named <code>Email Address</code> (Name property) that is configured to <code>Display to User</code> (checked). See also <a href="#">Chapter 13, "Managing External Applications."</a></p> <p>If your WebCenter application offers a self-registration page with the facility to email user ID information on request, then you must ensure that public credentials are configured for the external application selected here. If public credentials are <i>not</i> defined, then emails cannot be sent to users on their request. WebCenter Spaces offers this feature on its self-registration page.</p> |

- Specify LDAP connection details for the Active Directory server managing group space distribution lists. For detailed parameter information, see [Table 11–12, "LDAP Directory Server Configuration Parameters"](#).

This section applies to WebCenter Spaces (or custom WebCenter applications leveraging the WebCenter Spaces group space management feature). WebCenter applications support Microsoft Exchange where distribution lists are managed on an Active Directory server.

---

**Note:** Active Directory server details must be provided as part of the mail connection for *group space distribution lists* to work.

---

**Table 11–12 LDAP Directory Server Configuration Parameters**

| Field                        | Description   |
|------------------------------|---|
| LDAP Host                    | Enter the hostname of the machine where the LDAP directory server (Lightweight Directory Access Protocol) is running.   |
| LDAP Port                    | Enter the port on which the LDAP directory server listens.  |
| LDAP Base DN                 | Enter the base distinguished name for the LDAP schema. For example, <code>CN=Users,DC=oracle,DC=com</code> .  |
| LDAP Domain                  | <p>Enter the domain that will be appended to distribution list names</p> <p>In WebCenter Spaces, for example, if the domain value is set to <code>oracle.com</code>, then the Finance Project group space will maintain a distribution list named <code>FinanceProject@oracle.com</code>.</p> |
| LDAP Administrator User Name | <p>Enter the user name of the LDAP directory server administrator.</p> <p>A valid user with privileges to make entries into the LDAP schema.</p>  |
| LDAP Administrator Password  | <p>Enter the password for the LDAP directory server administrator.</p> <p>The password will be stored in a secured store.</p>   |

**Table 11–12 (Cont.) LDAP Directory Server Configuration Parameters**

| Field             | Description  |
|-------------------|--|
| LDAP Default User | Enter a comma-delimited list of user names to whom you want to grant moderation capabilities. These users become members of every group space distribution list that is created. The users specified must exist in the base LDAP schema (specified in the LDAP Base DN field). |
| LDAP Secured      | Indicate whether a secured connection (SSL) is required between the WebCenter application and the LDAP directory server.   |

8. Configure advanced options for the mail server connection. For details, see [Table 11–13, "Mail Server Connection - Advanced Configuration"](#).

**Table 11–13 Mail Server Connection - Advanced Configuration**

| Field                           | Description   |
|---------------------------------|---|
| Connection Timeout (in Seconds) | Specify a suitable timeout for the connection.<br><br>This is the length of time (in seconds) the WebCenter application waits for a response from the mail server before issuing a connection timeout message. The default is -1. When set to -1, the service default (10 seconds) applies. |

9. Optional parameters can be added to the mail server connection. For example, those listed in [Table 11–14, "Additional Mail Connection Properties"](#).

**Table 11–14 Additional Mail Connection Properties**

| Additional Connection Property | Description   |
|--------------------------------|---|
| Various IMAP properties        | Any valid IMAP connection property. For example, <code>mail.imap.connectionpoolsize</code> .<br><br>For all valid list of protocol properties, see your mail server documentation. For a list of standard IMAP properties, see the Java Mail APIs:<br><br><a href="http://java.sun.com/products/javamail/javadocs/com/sun/mail/imap/package-summary.html">http://java.sun.com/products/javamail/javadocs/com/sun/mail/imap/package-summary.html</a> |
| Various SMTP properties        | Any valid SMTP connection property. For example, <code>mail.smtp.timeout</code> .<br><br>For all valid list of protocol properties, see your mail server documentation. For a list of standard SMTP properties, see the Java Mail APIs:<br><br><a href="http://java.sun.com/products/javamail/javadocs/com/sun/mail/smtp/package-summary.html">http://java.sun.com/products/javamail/javadocs/com/sun/mail/smtp/package-summary.html</a>            |

If additional parameters are required to connect to the mail server, expand **Additional Properties** and enter details as required (see [Table 11–15, "Mail Connection - Additional Properties"](#)).

**Table 11–15 Mail Connection - Additional Properties**

| Field  | Description  |
|--------|--|
| Add    | <p>Click <b>Add</b> to specify an additional connection parameter:</p> <ul style="list-style-type: none"> <li>■ <b>Name</b> -Enter the name of the connection property.</li> <li>■ <b>Value</b> - Enter the default value for the property.</li> <li>■ <b>Is Property Secured</b> - Indicate whether encryption is required. When selected, the property value is stored securely using encryption.</li> </ul> <p>For example, select this option to secure the <code>admin.password</code> property where the value is the actual password.</p> |
| Delete | <p>Click <b>Delete</b> to remove a selected property.</p> <p>Select the correct row before clicking <b>Delete</b>.</p> <p>Note: Deleted rows appear disabled until you click <b>OK</b>.</p>  |

10. Click **OK** to save this connection.

11. To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."](#)

### 11.3.3.2 Registering Mail Servers Using WLST

Use the WLST command `createMailConnection` to create a mail server connection. For command syntax and examples, see "createMailConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

To configure the Mail service to use the new mail server connection as its default connection, set `default=true`. See also, [Section 11.3.4.2, "Choosing the Active \(or Default\) Mail Server Connection Using WLST."](#)

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

---



---

**Note:** To start using new connections you must restart the managed server on which the WebCenter application is deployed. See, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

---



---

## 11.3.4 Choosing the Active (or Default) Mail Server Connection

You can register multiple mail server connections with a WebCenter application but only one connection can be designated as the default connection.

For WebCenter Spaces and custom WebCenter applications, the *default connection* becomes the back-end mail server for:

- Mail task flows
- Group space distribution lists

This section contains the following subsections:

- [Choosing the Active \(or Default\) Mail Server Connection Using Fusion Middleware Control](#)
- [Choosing the Active \(or Default\) Mail Server Connection Using WLST](#)

### 11.3.4.1 Choosing the Active (or Default) Mail Server Connection Using Fusion Middleware Control

To change the default connection:

1. Login to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application:
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)
  - [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#)
2. Do one of the following:
  - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings > Service Configuration**.
  - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter > Service Configuration**.
3. From the list of services on the WebCenter Services Configuration page, choose **Mail Server**.  
The Manage Mail Server Connections table indicates the current active connection (if any).
4. Select the connection you want to make the active (or default) connection, and then click **Edit**.
5. Select the **Active Connection** check box.
6. Click **OK** to update the connection.
7. To start using the new default connection you must restart the managed server on which the WebCenter application is deployed. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."](#)

### 11.3.4.2 Choosing the Active (or Default) Mail Server Connection Using WLST

Use the WLST command `setMailConnection` with `default=true` to make an existing mail server connection the default connection for the Mail service. For command syntax and examples, see "setMailConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

A connection does not cease to be the default connection for the Mail service if you change the default argument from `true` to `false`.

To disable a mail connection, either delete it, make another connection the 'active connection', or use the `removeMailServiceProperty` command:

```
removeMailServiceProperty(appName='webcenter', property='selected.connection')
```

Using this command, connection details are retained but the connection is no longer named as an active connection. See also, "removeMailServiceProperty".

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

---



---

**Note:** To start using the active connection you must restart the managed server on which the WebCenter application is deployed. See, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

---



---

## 11.3.5 Modifying Mail Server Connection Details

You can modify mail server connection details at any time.

To start using updated mail connections you must restart the managed server on which the WebCenter application is deployed.

This section contains the following subsections:

- [Modifying Mail Server Connection Details Using Fusion Middleware Control](#)
- [Modifying Mail Server Connection Details Using WLST](#)

### 11.3.5.1 Modifying Mail Server Connection Details Using Fusion Middleware Control

To update mail server connection details:

1. Log in to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application:
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)
  - [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#)
2. Do one of the following:
  - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings > Service Configuration**.
  - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter > Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, choose **Mail Server**
4. Select the connection name, and click **Edit**.
5. Edit connection details, as required. For detailed parameter information, see [Table 11–11, "Mail Server Connection Parameters"](#).
6. Click **OK** to save your changes.
7. To start using updated connection details you must restart the managed server on which the WebCenter application is deployed. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."](#)

### 11.3.5.2 Modifying Mail Server Connection Details Using WLST

Use the WLST command `setMailConnection` to edit existing mail server connection details. For command syntax and examples, see "setMailConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

If additional parameters are required to connect to your mail server, use the `setMailConnectionProperty` command. For details, see "setMailConnectionProperty".

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)



---



---

**Note:** To start using the updated connections you must restart the managed server on which the WebCenter application is deployed. See, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

---



---

## 11.3.6 Deleting Mail Server Connections

You can delete mail server connections at any time but take care when deleting the active (or default) connection. If you delete the active connection, Mail task flows will work as they all require a back-end mail server.

When you delete a connection, consider deleting the external application associated with the mail server connection *if* the application's sole purpose was to support this connection. See [Section 13.4, "Deleting External Application Connections."](#)

This section contains the following subsections:

- [Deleting a Mail Connection Using Fusion Middleware Control](#)
- [Deleting a Mail Connection Using WLST](#)

### 11.3.6.1 Deleting a Mail Connection Using Fusion Middleware Control

To delete a mail server connection:

1. Login to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application:
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)
  - [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#)
2. Do one of the following:
  - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings > Service Configuration**.
  - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter > Service Configuration**.
3. From the list of services on the WebCenter Services Configuration page, choose **Mail Server**.
4. Select the connection name, and click **Delete**.
5. To effect this change you must restart the managed server on which the WebCenter application is deployed. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."](#)

---



---

**Note:** Before restarting the managed server, mark another connection as active; otherwise, the service will be disabled.

---



---

### 11.3.6.2 Deleting a Mail Connection Using WLST

Use the WLST command `deleteConnection` to remove a mail server connection. For command syntax and examples, see "deleteConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

### 11.3.7 Setting Up Mail Service Defaults

Use the WLST command `setMailServiceProperty` to set defaults for the Mail service:

- `mail.messages.fetch.size`: Maximum number of messages displayed in mail inboxes.

For command syntax and examples, see "setMailServiceProperty" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

### 11.3.8 Testing Mail Server Connections

Confirm that the mail server is up by connecting to the server using any client, such as Thunderbird or Outlook.

For Microsoft Exchange, go to **Administrative Tools - Services** to confirm that the following services are running (Status: Started):

- Microsoft Exchange IMAP4
- Simple Mail Transfer Protocol (SMTP)

## 11.4 Setting Up Connections for the Search Service

This section contains the following subsections:

- [What You Should Know About Oracle Secure Enterprise Search Connections](#)
- [Oracle Secure Enterprise Search Prerequisites](#)
- [Registering Oracle Secure Enterprise Search Services](#)
- [Choosing the Active Oracle Secure Enterprise Search Connection](#)
- [Modifying Oracle Secure Enterprise Search \(SES\) Connection Details](#)
- [Deleting Oracle Secure Enterprise Search \(SES\) Connections](#)
- [Testing Oracle Secure Enterprise Search \(SES\) Connections](#)

### 11.4.1 What You Should Know About Oracle Secure Enterprise Search Connections

The WebCenter Search service does not depend on Oracle Secure Enterprise Search (SES) to search for content created inside WebCenter applications by other WebCenter Web 2.0 services. However, you can extend WebCenter searches to external content repositories by connecting the WebCenter application to an Oracle SES instance.

Providing that the Oracle Secure Enterprise Search (SES) instance is set up to search repositories outside of Oracle WebCenter, results from these search sources can appear alongside WebCenter application search results.

Supported versions include Oracle Secure Enterprise Search 10.1.8.4 or later.

You can register multiple Oracle SES connections but only one of them is active at a time.

### 11.4.2 Oracle Secure Enterprise Search Prerequisites

This section contains the following subsections:

- [Oracle Secure Enterprise Search - Installation](#)
- [Oracle Secure Enterprise Search - Configuration](#)
- [Oracle Secure Enterprise Search - Security](#)
- [Oracle Secure Enterprise Search - Limitations](#)

#### 11.4.2.1 Oracle Secure Enterprise Search - Installation

For information on installation, see "Back-End Requirements for the Search Service" in *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*.

#### 11.4.2.2 Oracle Secure Enterprise Search - Configuration

Make sure you have a trusted federated entity on the Oracle SES instance for the current instance of WebCenter.

For secure searches, your WebCenter application and your Oracle SES instance must be using the same identity management system.

#### 11.4.2.3 Oracle Secure Enterprise Search - Security

See [Section 14.6.9, "Securing the WebCenter Spaces Connection to Oracle SES with SSL."](#)

#### 11.4.2.4 Oracle Secure Enterprise Search - Limitations

None.

### 11.4.3 Registering Oracle Secure Enterprise Search Services

You can register multiple SES connections with a WebCenter application but only one of them is active at a time.

To start using a new (active) Oracle SES connection you must restart the managed server on which the WebCenter application is deployed.

This section contains the following subsections:

- [Registering SES Search Services Using Fusion Middleware Control](#)
- [Registering SES Services Using WLST](#)

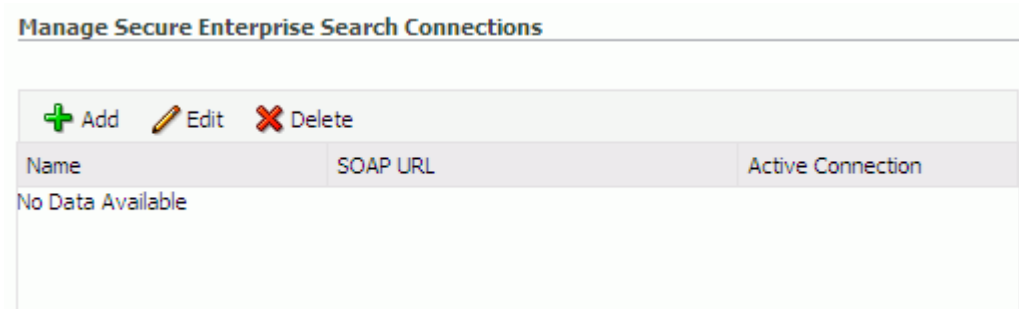
#### 11.4.3.1 Registering SES Search Services Using Fusion Middleware Control

To register an Oracle Secure Enterprise Search server with WebCenter Spaces:

1. Login to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application:
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)
  - [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#)
2. Do one of the following:
  - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings > Service Configuration**.
  - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter > Service Configuration**.

3. From the list of services on the WebCenter Service Configuration page, choose **Search**.
4. To connect to a new Oracle SES instance, click **Add** (Figure 11–8).

**Figure 11–8 Configuring Oracle Secure Search Services**



5. Enter a unique name for this connection, and indicate whether this connection is the active (or default) connection for the application.

See also, [Table 11–16, " Search Connection - Name"](#).

**Table 11–16 Search Connection - Name**

| Field             | Description  |
|-------------------|--|
| Name              | Enter a unique name for the connection. The name must be unique (across all connection types) within the WebCenter application.  |
| Active Connection | Select to use the SES instance defined on this connection to search repositories outside the WebCenter application and include Oracle SES search results in your result set. |

6. In the **Connection Name** field, enter a unique name for the search connection.
7. Enter connection details for the Oracle Secure Enterprise Search instance.

For detailed parameter information, see [Table 11–17, " Oracle Secure Enterprise Search - Connection Details"](#).

**Table 11–17 Oracle Secure Enterprise Search - Connection Details**

| Field    | Description  |
|----------|--|
| SOAP URL | Enter the Web Services URL that Oracle SES exposes to enable search requests.<br>Use the format:<br><code>http://&lt;host&gt;:&lt;port&gt;/search/query/OracleSearch</code><br>For example:<br><code>http://myHost:7777/search/query/OracleSearch</code> |

**Table 11–17 (Cont.) Oracle Secure Enterprise Search - Connection Details**

| Field                 | Description  |
|-----------------------|--|
| Application User Name | Enter the user name of the Oracle SES Federation Trusted Entity.<br><br><b>Tip:</b> This user is configured under Global Settings - Federation Trusted Entities (Oracle SES administration pages).<br><br>The user must be present in both the Oracle Identity Management server configured for your WebCenter application and the Oracle Identity Management server configured for Oracle SES.<br><br>The WebCenter application must authenticate itself as a trusted application to Oracle SES so that it may perform searches on behalf of WebCenter users. |
| Application Password  | Enter the appropriate user password.   |

8. Configure additional options for the Oracle Secure Enterprise Search connection.

---

**Note:** With the exception of the "Oracle Secure Enterprise Search Data Group" parameter, *configuration options are not specific to the current SES connection.*

---

For detailed parameter information, see [Table 11–18, "Oracle Secure Enterprise Search - Advanced Configuration"](#).

**Table 11–18 Oracle Secure Enterprise Search - Advanced Configuration**

| Field   | Description   |
|---|---|
| Oracle Secure Enterprise Search Data Group    | Specify the Oracle SES data group in which to search. If a value is not provided, then everything in the Oracle SES instance will be searched.                              |
| Execution Timeout                             | Enter the maximum time that a service is allowed to execute a search (in ms).   |
| Executor Preparation Timeout                  | Enter the maximum time that a service is allowed to initialize a search (in ms).  |
| Number of Saved Searches                      | Enter the number of saved searches displayed in the Saved Search drop down (on main search page).   |
| Results per Service - Saved Search Task Flows | Enter the number of search results displayed, per service, in a Saved Search task flow.   |
| Results per Service - Search Page             | Enter the number of search results displayed, per service, for searches submitted from the main search page.<br><br>Users can click <i>Show All</i> to see all the results. |
| Results per Service - Search Toolbar          | Enter the number of search results displayed, per service, for searches submitted from the global search toolbar.   |

9. Click **OK** to save this connection.
10. To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."](#)

### 11.4.3.2 Registering SES Services Using WLST

Use the WLST command `createSESConnection` to create a Oracle SES connection. Use `setSESConnection` to alter an existing Oracle SES connection. For command syntax and examples, see "createSESConnection" and "setSESConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

To configure the WebCenter Search service to actively use a new SES connection, set `default=true`. See also, [Section 11.4.4.2, "Choosing the Active Oracle Secure Enterprise Search \(SES\) Connection Using WLST."](#)

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

---



---

**Note:** To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed. See, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

---



---

## 11.4.4 Choosing the Active Oracle Secure Enterprise Search Connection

You can register multiple Oracle Secure Enterprise Search (SES) connections with a WebCenter application but only one connection is active at a time.

For WebCenter Spaces and any custom WebCenter application, the *active connection* becomes the back-end search engine for external content repositories.

This section contains the following subsections:

- [Choosing the Active Oracle Secure Enterprise Search \(SES\) Connection Using Fusion Middleware Control](#)
- [Choosing the Active Oracle Secure Enterprise Search \(SES\) Connection Using WLST](#)

### 11.4.4.1 Choosing the Active Oracle Secure Enterprise Search (SES) Connection Using Fusion Middleware Control

To change the active connection:

1. Login to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application:
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)
  - [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#)
2. Do one of the following:
  - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings > Service Configuration**.
  - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter > Service Configuration**.
3. From the list of services on the WebCenter Services Configuration page, choose **Search**.

The Manage Secure Enterprise Search Connections table indicates the current active connection (if any).

4. Select the connection you want to make the active (or default) connection, and then click **Edit**.
5. Select the **Active Connection** check box.
6. Click **OK** to update the connection.
7. To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."](#)

#### 11.4.4.2 Choosing the Active Oracle Secure Enterprise Search (SES) Connection Using WLST

Use the WLST command `setSESConnection` with `default=true` to activate an existing Oracle SES connection. For command syntax and examples, see "setSESConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

To subsequently disable an Oracle SES connection, run the same WLST command with `default=false`. Connection details are retained but the connection is no longer named as an active connection.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

---

**Note:** To start using the active connection you must restart the managed server on which the WebCenter application is deployed. See, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

---

### 11.4.5 Modifying Oracle Secure Enterprise Search (SES) Connection Details

You can modify Oracle SES connection details at any time.

To start using the updated (active) connection you must restart the managed server on which the WebCenter application is deployed.

This section contains the following subsections:

- [Modifying Oracle Secure Enterprise Search \(SES\) Connection Details Using Fusion Middleware Control](#)
- [Modifying Search Service Properties Using WLST](#)

#### 11.4.5.1 Modifying Oracle Secure Enterprise Search (SES) Connection Details Using Fusion Middleware Control

To update connection details for an Oracle Secure Enterprise Search instance:

1. Login to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application:
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)
  - [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#)
2. Do one of the following:
  - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings > Service Configuration**.

- For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter > Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, choose **Search**.
  4. Select the connection name, and click **Edit**.
  5. Edit connection details, as required. For detailed parameter information, see [Table 11–17, "Oracle Secure Enterprise Search - Connection Details"](#).
  6. Click **OK** to save your changes.
  7. To start using the updated (active) connection you must restart the managed server on which the WebCenter application is deployed. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."](#)

#### 11.4.5.2 Modifying Search Service Properties Using WLST

Use the WLST command `setSearchConfig` to edit properties relating to the Search service, such as the number of search results displayed. For command syntax and examples, see "setSearchConfig" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

---

---

**Note:** To start using updated properties you must restart the managed server on which the WebCenter application is deployed. See, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

---

---

#### 11.4.5.3 Modifying SES Connection Details Using WLST

Use the WLST command `setSESConnection` to edit an existing SES search connection. For command syntax and examples, see "setSESConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

Use the command `setSearchSESConfig` to set additional SES connection properties, such as the SES data group in which to search. For syntax details and examples, see "setSearchSESConfig".

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

---

---

**Note:** To start using the updated (active) connection you must restart the managed server on which the WebCenter application is deployed. See, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

---

---

### 11.4.6 Deleting Oracle Secure Enterprise Search (SES) Connections

You can delete Oracle SES connections at any time but take care when deleting the active connection. If you delete the active connection, users will not be able to search content on external repositories.

- [Deleting Search Connections Using Fusion Middleware Control](#)
- [Deleting Search Connections Using WLST](#)



### 11.4.6.1 Deleting Search Connections Using Fusion Middleware Control

To delete an Oracle Secure Enterprise Search server connection:

1. Login to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application:
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)
  - [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#)
2. Do one of the following:
  - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings > Service Configuration**.
  - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter > Service Configuration**.
3. From the Service Connection drop-down, choose **Search**.
4. Select the connection name, and click **Delete**.
5. To effect this change you must restart the managed server on which the WebCenter application is deployed. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments."](#)

### 11.4.6.2 Deleting Search Connections Using WLST

Use the WLST command `deleteConnection` to remove a search connection. For command syntax and examples, see "deleteConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

## 11.4.7 Testing Oracle Secure Enterprise Search (SES) Connections

Confirm the Oracle SES connection by entering the URL for Oracle SES Web Services operations: `http://<host>:<port>/search/query/OracleSearch`.

If the URL address does not render in the browser, then either the host or port for the Oracle SES server is incorrect or Oracle SES has not been started.

If the URL address does render in the browser, then select `proxyLogin` and click the link to start constructing a SOAP request for the operation. Enter the trusted federation entity user name and password, as well as a user name that is present in the identity management server used by Oracle SES. Click **Run** to execute the operation. Confirmation messages show that the connection is good.

## 11.5 Setting Up Connections for the Worklist Service

Several WebCenter services require a connection to a BPEL (Business Process Execution Language) server, namely, the Worklist, and WebCenter Spaces work flows. It's up to you whether these WebCenter services share the same connection or each connect to different BPEL servers.

- **Worklist service** -allows multiple connections so that WebCenter users can monitor and manage assignments and notifications from a range of BPEL servers. For details, see [Section 11.5.2, "Setting Up Worklist Connections"](#).

- **WebCenter Spaces workflows** - requires a single connection to the BPEL server included with the Oracle SOA Suite. For details, see [Section 9.1.1, "Specifying the BPEL Server Hosting WebCenter Spaces Workflows"](#).

This section includes the following sub sections:

- [BPEL Server Prerequisites](#)
- [Setting Up Worklist Connections](#)

## 11.5.1 BPEL Server Prerequisites

Consider the following to ensure smooth functioning of the Worklists service:

- Pages that include Worklists task flows must be secured through the ADF security.
- The Worklists service must be configured to an Oracle SOA Suite BPEL server, which is accessible through the BPEL Worklists application. The URL is in this format: `http://host:port/integration/worklistapp`. Users must be identical in both identity stores (LDAP).
- Clocks of the Worklists service's managed server and the Oracle SOA Suite BPEL's managed server must be in sync such that the SAML authentication condition, `NotBefore`, which checks the freshness of the assertion, is not breached.
- No configuration-related exceptions must exist. The WLST command `listWorklistConnections()` displays the configured connections, and therefore, can be used to validate that connection details.
- If the Oracle SOA Suite BPEL's managed server is configured to use a shared identity store and that store does not contain the user, `weblogic` by default, then the `weblogic` user must be configured, as described in [Appendix B.8.2.2, "Shared User Directory Does Not Include the weblogic User"](#).
- The `wsm-pm` applications must be running on both, the Worklists service's and Oracle SOA Suite's BPEL server's managed servers without any issues. This can be validated through the URL: `http://host:port/wsm-pm/validator`.

For information on how to resolve related issues, see [Section B.8, "Troubleshooting Worklist Service Issues"](#).

This section contains the following subsections:

- [BPEL Server - Installation and Configuration](#)
- [BPEL Server - Security Considerations](#)
- [BPEL Server - Limitations](#)

### 11.5.1.1 BPEL Server - Installation and Configuration

For installation and configuration-related information, see the section "Back-End Requirements for the Worklist Service and WebCenter Spaces Workflows" in *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*.

### 11.5.1.2 BPEL Server - Security Considerations

The Worklist service displays tasks for the currently authenticated user. For WebCenter users to store and retrieve tasks on the BPEL server, their user names need to either exist in a shared user directory (LDAP), or set up similarly (same user name and password) on both the WebCenter application and the BPEL Server.

For example, if the user `rsmith` want to use the Worklist service to store and retrieve tasks from the BPEL server, you must ensure that the user `rsmith` exists (with the same password) on both the BPEL server and within your application.

For a secured connection to the Worklist service, a shared Oracle Single Sign-On (OSSO) between the WebCenter application and the Oracle SOA Suite instance must be configured. For information, see [Section 14.7.2, "Configuring Oracle Single Sign-On \(OSSO\)."](#)

For information on configuring WS-Security between SOA and WebCenter Spaces, see [Section 14.8.1, "Securing the BPEL Server with WS-Security."](#)

### 11.5.1.3 BPEL Server - Limitations

None.

## 11.5.2 Setting Up Worklist Connections

This section contains the following subsections:

- [What You Should Know About Worklist Connections](#)
- [Registering Worklist Connections](#)
- [Activating a Worklist Connection](#)
- [Modifying Worklist Connection Details](#)
- [Deleting Worklist Connections](#)
- [Testing Worklist Connections](#)

### 11.5.2.1 What You Should Know About Worklist Connections

The Worklist service enables WebCenter applications to show authenticated users a list of BPEL worklist items currently assigned to them through the Worklist task flow. BPEL worklist items are open BPEL tasks from one or more BPEL worklist repository.

A connection to every BPEL server that must delivering worklist items is required. Multiple worklist connections are allowed so that WebCenter users can monitor and manage assignments and notifications from a range of BPEL servers.

Worklist connection details are stored in `connections.xml`. Another file, `adf-config.xml`, identifies which connections are actively used by the Worklist service.

If, for any reason, a BPEL server cannot be contacted, the Worklist will indicate that the connection is unavailable.

### WebCenter Spaces

The WebCenter Spaces application requires a BPEL server connection to support its internal workflows, that is, group space membership notifications and group space subscription requests. The BPEL server providing this functionality is always a BPEL server included with the Oracle SOA Suite. See also, [Specifying the BPEL Server Hosting WebCenter Spaces Workflows](#).

The Worklist service can share the SOA instance connection and by doing so, display worklist items relating to group space activity in each user's Worklist task flow.

### 11.5.2.2 Registering Worklist Connections

This section contains the following subsections:

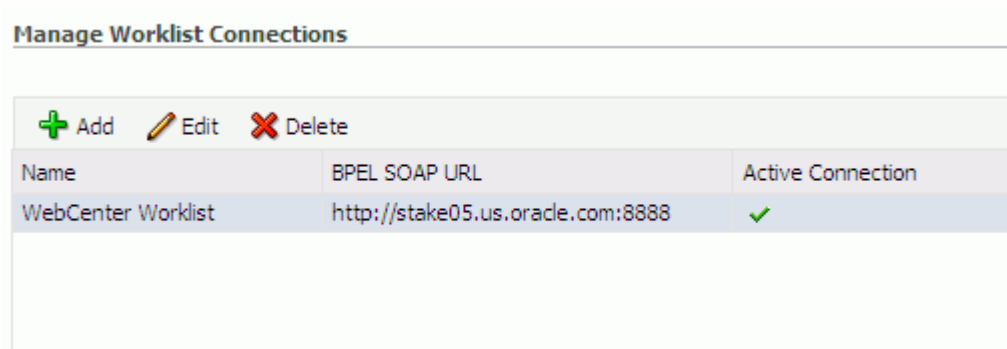
- [Registering Worklist Connections Using Fusion Middleware Control](#)
- [Registering Worklist Connections Using WLST](#)

**11.5.2.2.1 Registering Worklist Connections Using Fusion Middleware Control**

To register a Worklist connection:

1. Login to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application:
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)
  - [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#)
2. Do one of the following:
  - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings > Service Configuration**.
  - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter > Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, choose **Worklist**.
4. To register a new connection, click **Add** ([Figure 11-9](#)).

**Figure 11-9 Configuring Worklist Connections**



5. Enter a unique name for the Worklist connection and activate the connection if you want to use the connection immediately.

See also, [Table 11-19, " Worklist Connection - Name"](#).

**Table 11-19 Worklist Connection - Name**

| Field | Description   |
|-------|---|
| Name  | <p>Enter a unique name for the connection. The name must be unique (across all connection types) within the WebCenter application.</p> <p>This name may be displayed to users working with the worklist feature in the WebCenter application. Users may organize their worklist assignments through various sorting and grouping options. The option "Group By Worklist Server" displays the name you specify here so it's important to enter a meaningful name that other users will easily recognize, for example, Human Resources.</p> |

**Table 11–19 (Cont.) Worklist Connection - Name**

| Field             | Description  |
|-------------------|--|
| Active Connection | <p>(Select to activate this worklist connection in the WebCenter application. Once activated, worklist items from the associated BPEL server display in users' worklists.</p> <p>Multiple worklist connections may be active at a time, enabling WebCenter users to monitor and manage assignments and notifications from a range of BPEL servers. If you need to disable a connection for any reason, deselect this option.</p> <p>(Edit mode only.) Check boxes indicate whether other components share this connection:</p> <ul style="list-style-type: none"> <li>■ <b>WebCenter Spaces Application</b> <p>Indicates whether WebCenter Spaces uses the same BPEL server connection for internal workflows, such as Group Space membership notifications, Group Space subscription requests, and more. The BPEL server that provides this functionality is the BPEL server included with the Oracle SOA Suite. See also, <a href="#">Section 9.1.1, "Specifying the BPEL Server Hosting WebCenter Spaces Workflows"</a>.</p> <p>Before modifying connection properties, consider impact to any other components that share this connection.</p> </li> </ul> |

6. Enter connection details for the BPEL server.

For details, see [Table 11–20, "Worklist Connection - Connection Details"](#).

**Table 11–20 Worklist Connection - Connection Details**

| Field         | Description  |
|---------------|--|
| BPEL Soap URL | <p>Enter the URL required to access the BPEL server.</p> <p>Use the format: &lt;protocol&gt;://&lt;host&gt;:&lt;port&gt;</p> <p>For example, <code>http://mybpelsever.com:8001</code></p> <p>The URL must be unique within the WebCenter application.</p> <p>Note: WebCenter Spaces uses the BPEL server included with the Oracle SOA Suite to implement group space subscription workflows. When setting up this connection, make sure you enter the SOA Suite's BPEL server URL here. See also, <a href="#">Section 9.1.1, "Specifying the BPEL Server Hosting WebCenter Spaces Workflows"</a></p> |

**Table 11–20 (Cont.) Worklist Connection - Connection Details**

| Field                 | Description   |
|-----------------------|---|
| SAML Token Policy URI | <p>Select the SAML token policy this connection uses for authentication.</p> <p>SAML (Security Assertion Markup Language) is an XML-based standard for passing security tokens defining authentication and authorization rights. An attesting entity (that already has trust relationship with the receiver) vouches for the verification of the subject by method called sender-vouches.</p> <p>Options available are:</p> <ul style="list-style-type: none"> <li>▪ <b>SAML Token Client Policy</b> (oracle/wss10_saml_token_client_policy) - Select to verify your basic configuration without any additional security. This is the default setting.</li> <li>▪ <b>SAML Token With Message Client Policy</b> (oracle/wss10_saml_token_with_message_protection_client_policy) - Select to increase the security using SAML-based BPEL Web Services. If selected, you must configure keys stores both in your WebCenter application and in the BPEL application.</li> </ul> |

7. Click **OK** to save this connection.
8. To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments"](#).

#### 11.5.2.2.2 Registering Worklist Connections Using WLST

Use the WLST command `createBPELConnection` to create a BPEL server connection. For command syntax and examples, see "createBPELConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

To configure the Worklist service to actively use a new BPEL server connection some additional configuration is required. See, [Section 11.5.2.3.2, "Activating a Worklist Connections Using WLST"](#).

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands"](#).

---

**Note:** To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed. See, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

---

#### 11.5.2.3 Activating a Worklist Connection

In WebCenter applications, multiple Worklist connections may be active at a time. This enables WebCenter users to monitor and manage assignments and notifications from a multiple BPEL servers. From time to time you may need to temporarily disable an active connection, or reactive a connection.

This section contains the following subsections:

- [Activating a Worklist Connections Using Fusion Middleware Control](#)
- [Activating a Worklist Connections Using WLST](#)

##### 11.5.2.3.1 Activating a Worklist Connections Using Fusion Middleware Control

To activate or disable a Worklist connection:

1. Login to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application:
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)
  - [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#)
2. Do one of the following:
  - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings > Service Configuration**.
  - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter > Service Configuration**.
3. From the list of services on the WebCenter Services Configuration page, choose **Worklist**.  
The Manage Worklist Connections table indicates currently active connections (if any).
4. Select the Worklist connection you want to activate (or disable), and then click **Edit**.
5. Select the **Worklist** check box to activate this Worklist connection in the WebCenter application.  
Once activated, worklist items from the associated BPEL server display in Worklist task flows. If you need to disable a connection for any reason, deselect this option.
6. Click **OK** to update the connection.
7. To start using the new (active) connection you must restart the managed server on which the WebCenter application is deployed. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments"](#).

#### 11.5.2.3.2 Activating a Worklist Connections Using WLST

Use the WLST command `addWorklistConnection` to activate an existing BPEL connection for Worklist services. For command syntax and examples, see "addWorklistConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

To subsequently disable a BPEL connection used by the Worklist service, run the WLST command `removeWorklistConnection`. Connection details are retained but the connection is no longer named as an active connection. For syntax details and examples, see "removeWorklistConnection".

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands"](#).

---

**Note:** To start using the active connection you must restart the managed server on which the WebCenter application is deployed. See, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

---

#### 11.5.2.4 Modifying Worklist Connection Details

This section contains the following subsections:



- [Modifying Worklist Connection Details Using Fusion Middleware Control](#)
- [Modifying Worklist Connection Details Using WLST](#)

#### 11.5.2.4.1 Modifying Worklist Connection Details Using Fusion Middleware Control

To update worklist connection details:

1. Login to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application:
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)
  - [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#)
2. Do one of the following:
  - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings > Service Configuration**.
  - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter > Service Configuration**.
3. From the list of services on the WebCenter Services Configuration page, choose **Worklist**.
4. Select the Worklist connection you want to activate, and then click **Edit**.
5. Edit connection details, as required. For detailed parameter information, see [Table 11–20, "Worklist Connection - Connection Details"](#).
6. Click **OK** to update the connection.
7. To start using the updated (active) connection you must restart the managed server on which the WebCenter application is deployed. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments"](#).

#### 11.5.2.4.2 Modifying Worklist Connection Details Using WLST

Use the WLST command `setBPELConnection` to edit existing BPEL server connection details. For command syntax and examples, see "setBPELConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands"](#).

---

---

**Note:** To start using the updated (active) connection you must restart the managed server on which the WebCenter application is deployed. See, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

---

---

#### 11.5.2.5 Deleting Worklist Connections

Before you delete a Worklist connection, check to see whether the WebCenter Spaces workflows, use the same connection.

This section contains the following subsections:

- [Deleting Worklist Connections Using Fusion Middleware Control](#)
- [Deleting Worklist Connections Using WLST](#)

##### 11.5.2.5.1 Deleting Worklist Connections Using Fusion Middleware Control



To delete a worklist connection:

1. Login to Fusion Middleware Control and navigate to the home page for WebCenter Spaces or the custom WebCenter application:
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)
  - [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#)
2. Do one of the following:
  - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings > Service Configuration**.
  - For WebCenter applications - From the **Application Deployment** menu, choose **WebCenter > Service Configuration**.
3. From the list of services on the WebCenter Services Configuration page, choose **Worklist**.
4. Select the Worklist connection you want to delete, and then click **Delete**.
5. To confirm, click **Yes**.
6. To effect this change you must restart the managed server on which the WebCenter application is deployed. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments"](#).

#### 11.5.2.5.2 Deleting Worklist Connections Using WLST

Use the WLST command `deleteConnection` to remove a BPEL connection previously registered for the Worklist service. For command syntax and examples, see "deleteConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands"](#).

#### 11.5.2.6 Testing Worklist Connections

Log in to the SOA BPEL Worklist application with valid user credentials. A Worklist application is accessible through the URL in the following format:

```
protocol://host:port/integration/worklistapp
```

For example, `http://mybpelserver.com:8001/integration/worklistapp`.

You can also verify the status of the `wsm-pm` application, which manages the SAML policy web service authentication mechanism used by Worklist. To show the list of `wsm-pm` policies, log in to both, the SOA BPEL server and the server running the Worklist task flow using the following URL format:

```
protocol://SOA_server_host:port/wsm-pm/validator
```

For example, `http://mybpelserver.com:8001/wsm-pm/validator` and `http://myWorklistHostingServer.com:8888/wsm-pm/validator`.

## 11.6 Setting Up the WebCenter Repository

WebCenter Web 2.0 services, such as Group Space Events, Links, Lists, and Tags, store information in WebCenter repository, which uses an Oracle Database. [Table 11–21](#)

describes what information each service stores in the WebCenter repository. See also, *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

For information on backing up and migrating this information, see [Chapter 16, "Managing Export, Import, Backup, and Recovery of WebCenter"](#).

**Table 11–21 WebCenter Web 2.0 Services Storing Content in WebCenter Repository**

| WebCenter Web 2.0 Services | Description   | Content Stored in WebCenter Repository   | WebCenter Spaces | Custom WebCenter application |
|----------------------------|---|--|------------------|------------------------------|
| Group Space Events         | Scheduled appointments, meetings, presentations, or any other kind of gathering for a particular group space.<br><br>Group space members can view such events on the group space's dedicated Events page or in any Events task flow that is located on a page in the group space. | Group space event details, such as, meetings, appointments, presentations, and so on.            | Yes              | No                           |
| Links                      | Links connect different pieces of previously unlinked information, producing context between items. As users build webs of related information, this knowledge can be communicated to the wider group.  | Link maps, that is, relationship information such as what object is linked to what other object. | Yes              | Yes                          |
| Lists                      | Enables users to track issues, capture project milestones, publish project assignments, and so on.  | List data, that is, column values in List rows.  | Yes              | No                           |
| Tags                       | Allows users to apply their own meaningful terms to items, making those items more easily discoverable in search results and the Tag Center - a dynamically generated page that displays all the tags users have added.   | Resources, bookmarks created on resources, and tag words used in each bookmark.                  | Yes              | Yes                          |

A WebCenter repository for WebCenter Spaces is configured out-of-the-box, and therefore, the repository connection does not require reconfiguration.

To enable Web 2.0 Services in a custom WebCenter application you need to set up a connection to the WebCenter repository (the database where the WebCenter schema is installed). The WebCenter schema is included with the product. To install the WebCenter schema, follow the steps described in "Installing Oracle WebCenter" in *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*.

For custom WebCenter applications, developers first create a database connection in Oracle JDeveloper, as described in the section "Creating a Database Connection" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*. This database connection can be of types: **JDBC DataSource** or **JDBC URL**. For information on different types of data sources, see the section "What You May Need to Know About Database Connections and Application Security Migration When Deploying WebCenter Applications" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

Depending on the connection type used in an application, do one of the following:

- Create a global data source, if the application does not include an application-level data source with password indirection. For information on creating global data sources, see the section "Creating a JDBC Data Source" in *Oracle Fusion Middleware Configuring and Managing JDBC for Oracle WebLogic Server*.
- Map the connection credentials, if the application uses an application-level data source with password indirection. The password is set through the Oracle WebLogic Administration Console on the **Credential Mappings** tab under **Security**. If you change the password for an indirect data source on the **Connection Pool** tab under **Configuration**, then it will have no effect. For more information on credential mapping, see "JDBC Data Sources: Security: Credential Mapping" under the section "Creating a JDBC Data Source" in *Oracle Fusion Middleware Configuring and Managing JDBC for Oracle WebLogic Server*.
- Merge the information stored in application credential store with that of the global application store, if the application uses a JDBC URL connection. For more information on credential migration behavior, see the section "Configuring the Credential Store" in *Oracle Fusion Middleware Security Guide*.

In a typical business scenario, applications are deployed to different managed servers and multiple databases are used as repositories for the applications. The repository that you use in a development environment is different from that in a production environment, and therefore, when migrating custom WebCenter applications from development to production, you need to reconfigure the database connection.

When a repository connection is reconfigured, the local `datasource` file and the `*-jdbc.xml` file in the `WEB-INF` directory of the WAR file are updated with the new connection details. However, the `JNDI Name` and `data source` name remain the same. If you change `JNDI Name` for any reason, then you must also update the `adf-config.xml` file. The `JNDI name` must be of the form `jdbc/connection-nameDS`. For example, if the application has a connection name `connection1`, the `JNDI name` is `jdbc/connection1DS`.

## 11.7 Setting Up the MDS Repository

WebCenter Web 2.0 services, such as Notes, RSS News Feed, Recent Activities, Worklists, Search, Page, and Mail store information in the MDS repository. To enable these services in a WebCenter applications you need to configure the MDS repository.

For information on creating a MDS repository or configuring an existing WebCenter application to use a different MDS repository or partition, see section "Managing the Oracle Metadata Repository" in *Oracle Fusion Middleware Administrator's Guide*.

## 11.8 Setting Up the Server for Wiki and Blog Services

Oracle WebCenter Wiki and Blog Server enables you to integrate wikis and blogs into your WebCenter applications. A wiki is a type of web site where users can browse available content and update and remove content, sometimes without the need for registration. This ease of interaction and the variety of operations makes wiki an effective tool for collaborative authoring, where multiple people create written content together using the wiki markup language.

To use wikis and blogs in your applications, you must deploy Oracle WebCenter Wiki and Blog Server to Oracle WebLogic Server. For information, see *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*.

This section describes the basic administration and configuration tasks that can be performed on a wiki and blog server. Note that you may need to perform only some of these tasks, depending on your requirements.

- [What You Should Know About the Wiki and Blog Server Interface](#)
- [Accessing Oracle WebCenter Wiki and Blog Server](#)
- [Setting Up Domains and Menus](#)
- [Changing the Theme](#)
- [Creating a User Interface Template](#)
- [Unlocking a Page](#)
- [Setting Up Server Security](#)
- [Managing Users and Roles](#)
- [Enabling Anonymous Access](#)
- [Blocking an IP Address](#)
- [Deleting Wiki Pages and Blog Entries](#)
- [Specifying Configuration Parameters](#)
- [Configuring Wiki Repository](#)
- [Specifying Features Supported on the Wiki and Blog Server](#)
- [Monitoring Oracle WebCenter Wiki and Blog Server](#)
- [Backing Up and Restoring Wiki Content](#)

### 11.8.1 What You Should Know About the Wiki and Blog Server Interface

When you log on to your wiki and blog server, the default wiki domain is displayed. The wiki and blog server also displays a toolbar of useful links across the top of the page, a search feature, a domain-specific menu on the navigation panel on the left, and additional navigation under the **General** heading, as shown in [Figure 11-10](#).

For administrators, the wiki and blog server displays an extra **Administration** link on the top header.

---

---

**Note:** The wiki and blog server provides the **logout** link. The link can be customized to any URL based on the single sign-on scheme used. To customize the link, you can modify the `logout_url` variable in the `application_config.script` file. Leaving `logout_url` blank renders the user session invalid and redirects to the login screen.

The `application_config.script` file is available at the following location:

```
$WLS_HOME/user_projects/domains/owc_wiki/servers/wiki_server/stage/11.1.1.1.0/owc_wiki/WEB-INF/classes
```

Where, *\$WLS\_HOME* is the Oracle WebLogic Server installation directory, *owc\_wiki* refers to the wiki and blog server domain, *wiki\_server* refers to the server to which the wiki and blog application is deployed, and *owc\_wiki* refers to the wiki and blog server deployment directory.

---

---

**Figure 11–10 Oracle WebCenter Wiki and Blog Server Interface**


---

**Note:** The supported browsers for Oracle WebCenter Wiki and Blog Server are Internet Explorer 7.0 or later, Mozilla Firefox 2.0 or later, and Apple Safari 4.0 or later.

---

### 11.8.1.1 About the General Menu

The General menu is a default menu and cannot be edited. You use the General menu to perform common operations on your wiki and blog server.

Table 11–22 describes the links available in the General menu of a domain.

**Table 11–22 Links in the General Menu**

| Link               | Description  |
|--------------------|--|
| All Pages          | Displays a list of all wiki pages in the current domain.   |
| All Blogs          | Enables you to view a list of all personal and domain blogs. You can access different blogs to add blog entries and manage blog authors. |
| Domain Information | Summarizes useful information about the current domain, such as details about popular pages and recently updated pages.                  |
| Recently Changed   | Displays a list of recently updated wiki pages.  |
| Popular Pages      | Displays a list of wiki pages, in the current domain, with the most number of page views.  |
| New Wiki Page      | Enables you to create a new wiki page in the current domain.   |

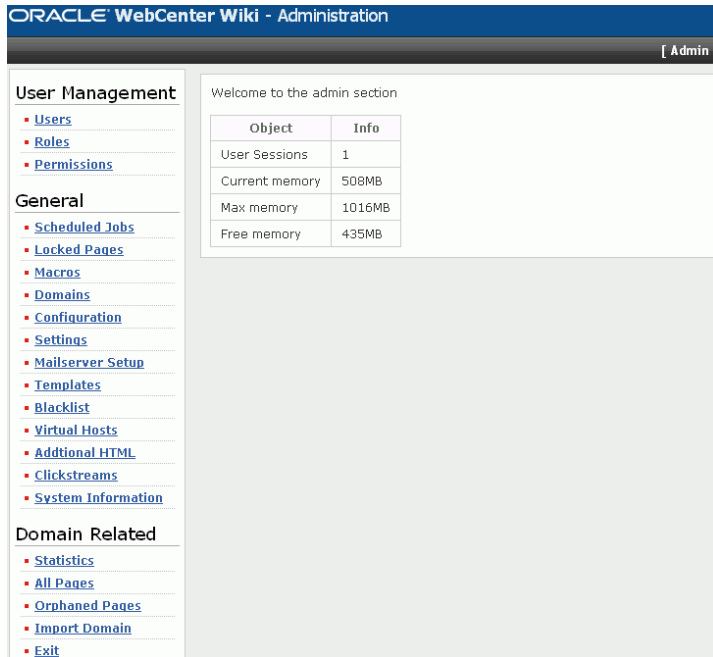
### 11.8.1.2 About the Administration Mode

To configure your wiki and blog server, you use the Administration mode of the server. You access the Administration mode by clicking the **Administration** link on your wiki and blog server. (Figure 11–11)

**Figure 11–11 Administration Link**

Figure 11–12 displays the Administration mode.

**Figure 11–12 Administration Mode**



The Administration mode contains various links that you can use to configure settings specific to the current domain or the entire wiki and blog server. [Table 11–23](#) describes the links available in the Administration mode.

**Table 11–23 Links in the Administration Mode of Oracle WebCenter Wiki and Blog Server**

| Link                   | Description  |
|------------------------|--|
| <b>User Management</b> |  |
| Users                  | Displays details, such as the name, e-mail address, status, and role of all wiki users. You can use this link to add new users, block or unblock users, reset their password, and edit their profile to assign them different roles. For more information, see <a href="#">Section 11.8.8.1, "Managing Users."</a><br><br><b>Note:</b> When you deploy the wiki and blog server by leveraging single sign-on security, users are not initially imported from the security store. A user entry is created on the wiki and blog server only upon first login by that user. |
| Roles                  | Enables you to add a new role and edit a role to manage permissions.<br><br>For information about how to assign permissions to a role, see <a href="#">Section 11.8.8.2, "Managing Permissions for a Role."</a>  |
| Permissions            | Displays a list of permissions that you can assign to various roles.   |
| <b>General</b>         |  |
| Scheduled Jobs         | Enables you to view administrative jobs that can be run, such as DailyIndexerJob for updating the search index. It also shows the next time each job is scheduled to run.<br><br>If you wish a job to run sooner, you can click the <b>run now</b> link.   |

**Table 11–23 (Cont.) Links in the Administration Mode of Oracle WebCenter Wiki and Blog Server**

| Link               | Description  |
|--------------------|--|
| Locked Pages       | <p>Displays details of pages that have been locked. These details include name of the user who locked the page, the time when the page was locked, and the time when the page will get unlocked automatically.</p> <p>To unlock a page, you can either wait for the time of the automatic unlock, or as an administrator, you can manually unlock a page by clicking the <b>remove lock</b> link.</p> <p>For information about how to unlock a page, see <a href="#">Section 11.8.6, "Unlocking a Page."</a></p> |
| Macros             | <p>Enables you to execute complex or specialized functions on a wiki page. You can invoke a macro by using the <code>&lt;macro:&gt;</code> tag. The wiki and blog server includes several sample macros, such as TaskMacro and Link. The Macro page provides a list and description of all sample macros.</p>  |
| Domains            | <p>Displays a list of all domains and their details, such as page counts and name of the start page. It also displays the total number of domains and pages on your wiki and blog server.</p> <p>You can use the Domains link to add or delete a domain, edit the details of a domain, and specify the members who can manage a domain. For information about how to manage domains, see <a href="#">Section 11.8.3, "Setting Up Domains and Menus."</a></p>   |
| Configuration      | <p>Enables you to configure your wiki and blog server by specifying details such as your default domain and wiki page, wiki repository, and wiki theme.</p> <p>For more information, see <a href="#">Section 11.8.12, "Specifying Configuration Parameters."</a></p>   |
| Settings           | <p>Enables you to specify your wiki and blog server settings. You can specify details such as whether attachments, self-registration of users, page ratings, and trackbacks are supported.</p> <p>For more information, see <a href="#">Section 11.8.14, "Specifying Features Supported on the Wiki and Blog Server."</a></p>  |
| Templates          | <p>Enables you to add, view, edit, and delete templates used for creating wiki pages.</p> <p>For more information, see <a href="#">Section 11.8.5, "Creating a User Interface Template."</a></p>   |
| Blacklist          | <p>Enables you to block certain IP addresses from adding or editing pages on your wiki and blog server. However, a blocked IP address can access the server to view pages.</p> <p>For more information, see <a href="#">Section 11.8.10, "Blocking an IP Address."</a></p>   |
| Virtual Hosts      | <p>Enables you to create multiple sites within the wiki and blog server differentiated by their host names.</p>  |
| Additional HTML    | <p>Enables you to define the additional HTML header and footer information that appears on every wiki page.</p>  |
| Clickstreams       | <p>Enables you to monitor the pages or functions that different users have accessed or clicked. Users are identified by their IP addresses, and the wiki or blog URL that they accessed is shown.</p>  |
| System Information | <p>Displays the version number for the wiki and blog server. The version is the open source version number. The Build option refers to the Oracle version and the build number.</p>  |

**Table 11–23 (Cont.) Links in the Administration Mode of Oracle WebCenter Wiki and Blog Server**

| Link                  | Description  |
|-----------------------|--|
| <b>Domain Related</b> |  |
| Statistics            | Displays statistics of the current domain for the specified time period. Domain statistics include names of wiki pages viewed, the page view count, and the dates on which pages were last viewed within the specified date range.   |
| All Pages             | Displays details of all the pages within the current domain. You can use this link to delete wiki pages. You can also choose to easily delete all wiki pages that do not contain any content.<br><br>For more information, see <a href="#">Section 11.8.11, "Deleting Wiki Pages and Blog Entries."</a>  |
| Orphaned Pages        | Displays the pages that are not linked to any other page.  |
| Export Domain         | Enables you to publish wiki pages in a domain as HTML files so that the pages can be placed on a web server and accessed directly.<br><br><b>Note:</b> By default, the Export Domain link is not available. To access this link, you must enable the <b>ExportDomain</b> permission for the ADMIN role.  |
| Import Domain         | Enables you to point to a directory containing wiki pages, like wiki pages of the 10.1.3.2 version of the wiki and blog server, and import the domain into the database-based repository.<br><br>For information about importing domains, see the "How to Migrate Wiki Data" section in the <i>Oracle Fusion Middleware Upgrade Guide for Oracle SOA Suite, WebCenter, and ADF</i> . |
| Exit                  | Exits the Administration mode.   |

## 11.8.2 Accessing Oracle WebCenter Wiki and Blog Server

You can access Oracle WebCenter Wiki and Blog Server by using the following URL format:

```
http://host:port/owc_wiki
```

Where *host:port* refer to the host and the port number of the server where you deployed Oracle WebCenter Wiki and Blog Server, and *owc\_wiki* refers to your deployed application. For example, if the managed server where you deployed the wiki and blog server is running on port 8001, you can access the wiki and blog server by using the following path: `http://localhost:8001/owc_wiki`.

## 11.8.3 Setting Up Domains and Menus

Domains are an organizing model on the wiki and blog server similar to folders on a file system. A wiki domain encompasses an identified group of wiki pages. It helps you organize wiki pages and secure them by role or specific users. Each wiki domain contains an associated blog, where blog authors can create blog entries and users can post comments.

As a wiki administrator, you can create, edit, or delete domains and manage domain members and blog authors. You can also create and edit domain menus to enable easy access to pages within each domain. This section discusses basic domain and menu administration tasks.

- [Adding a Domain](#)



- [Editing a Domain Menu](#)
- [Managing Domain Members](#)
- [Managing Blog Authors](#)

### 11.8.3.1 Adding a Domain

To create a new domain:

1. Log on to Oracle WebCenter Wiki and Blog Server as an administrator and access the Administration mode.
2. Under **General** in the navigation panel on the left, click **Domains**.  
The Domains page lists all the domains on the wiki and blog server.
3. Click **add** to create a new domain.
4. Enter a domain name, a description, and a name for the start page of your domain, as shown in [Figure 11–13](#).

**Figure 11–13 Adding a New Domain**

Add domain

Name:

Description:

Startpage :

5. Click **Save**.  
The newly created domain is listed on the Domains page, as shown in [Figure 11–14](#).

**Figure 11–14 List of Domains**

| [ Domains ]         |  |                             |            |                              |                      |                        |                                |
|---------------------|--|-----------------------------|------------|------------------------------|----------------------|------------------------|--------------------------------|
| <a href="#">add</a> |  |                             |            |                              |                      |                        |                                |
| Name                | Description                              | Startpage                   | Page Count | Created                      | Actions              |                        |                                |
| owc_wiki            | All about owc_wiki                       | <a href="#">WelcomePage</a> | 13         | fmwadmin at 10/14/2008 17:23 | <a href="#">edit</a> | <a href="#">delete</a> | <a href="#">manage members</a> |
| Seattle             | Wiki Domain For Seattle Support Training | <a href="#">SeattleHome</a> | 2          | fmwadmin at 12/25/2008 22:27 | <a href="#">edit</a> | <a href="#">delete</a> | <a href="#">manage members</a> |

6. To navigate directly to the new domain, click its start page link in the **Startpage** column.  
To exit the Administration mode, under **General**, click **Exit**. This displays the wiki page of the last domain that you accessed before entering the Administration mode.

---

---

**Note:** You can also create a domain by using the `scope` parameter in a wiki URL in any WebCenter application. If the specified domain does not exist, it is automatically created with the name specified in the `scope` parameter. The parameter also creates a start page named `WelcomePage`. For more information, see the "Integrating Oracle WebCenter Wiki and Blog Server" chapter in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

---

---

After creating a new domain, you can create wiki pages and blog entries in the domain. For information, see the "Working with Wikis and Blogs" chapter in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

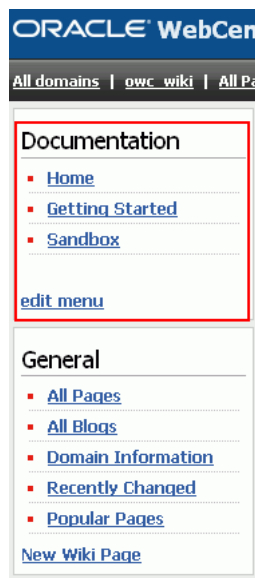
### 11.8.3.2 Editing a Domain Menu

As an administrator, you can create or edit the menu of a domain. The domain-specific menu appears at the top in the navigation panel. [Figure 11-15](#) shows the menu of the default domain, `owc_wiki`.

A menu comprises menu topics, which display as headers. Menu topics contain menu items. For example, in the `owc_wiki` domain, **Documentation** is a menu topic and **Home** is a menu item. Menu topics display on the navigational panel in the order in which you create them.

A newly created domain contains an empty wiki page named `Menu`. You use this page to create or edit the domain-specific menu. You can edit the `Menu` wiki page by using the **edit menu** link on the navigation panel.

**Figure 11-15** Domain Menu



---

**Note:** You can configure your wiki and blog server to display the required wiki management tools. You use the query string parameter `inline` to control how much wiki capability to render. On the wiki and blog server, the navigation panel on the left and the Menu wiki page appear when `inline=0`. The **edit menu** link appears only when `inline=0` and the user is an administrator.

When using `inline=1`, the Menu wiki page does not appear. Instead a menu is auto-generated showing all wiki pages in the domain. For information about inline modes, see the "Integrating Oracle WebCenter Wiki and Blog Server" chapter in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

---

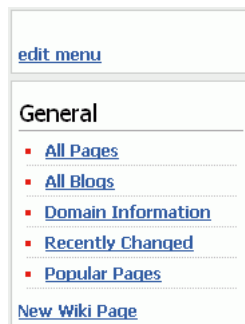
To modify the menu of a domain:

1. Click the **All domains** link on the toolbar of links on the top-left corner of your wiki and blog server user interface.  
Note that you do not need to access the Administration mode to edit a domain menu.
2. Click the start page link of the domain for which you wish to edit the menu.
3. Click the **edit menu** link. [Figure 11–16](#) shows the blank menu of a newly created domain.

The Edit Page displays.

**Tip:** You can also access the Edit Page by clicking **All Pages** under **General** on the navigation panel. This displays a list of all wiki pages of the current domain. You can click the **Menu** wiki page to view the menu, and then click the **Edit** tab to edit the menu.

**Figure 11–16** *Menu of a New Domain*



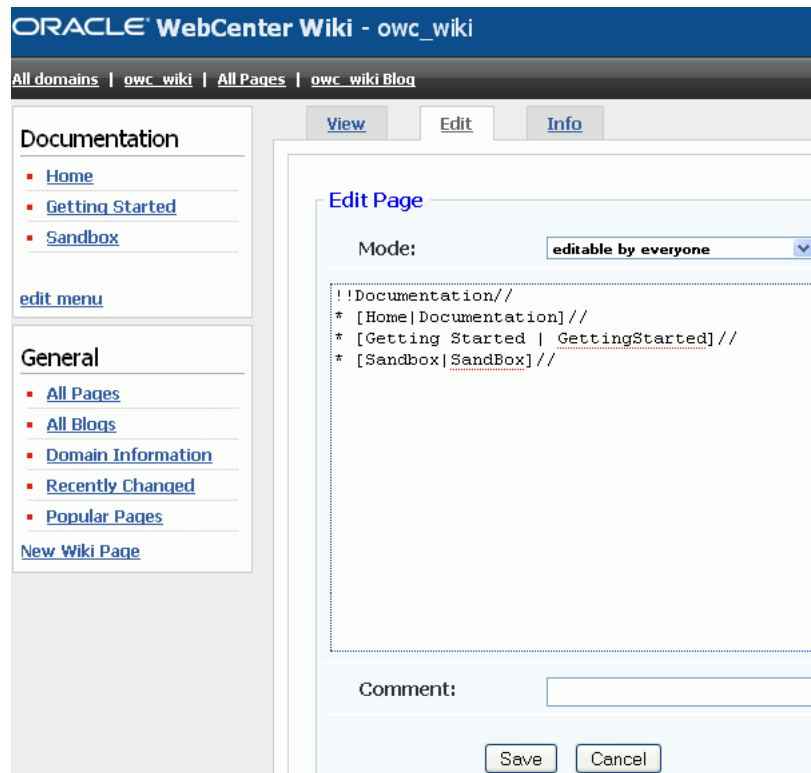
4. Specify the menu topic and menu items that you want to add or change. You can edit the menu the same way you edit a wiki page.

Within each menu topic, you can define menu items and link them to the required wiki pages or to the targets that are external to your wiki and blog server. When you create a menu item, you must provide a name and specify either the name of a wiki page or a URL. The name that you specify displays in the menu on the navigation panel.

**Tip:** When naming your page, ensure that you adhere to wiki markup standards, that is, you use the camel case notation for naming wiki pages. This notation uses an initial uppercase letter followed by lowercase letters, then another uppercase letter, and another series of lowercase letters, for example, MyWikiPage. To use an alternate name for your page, use the following convention: [alternate name | Wiki page name]. For example: [ My Page | MyPage ].

For information about wiki markup language to format page content, see the "Using Wiki Mark-Up" section in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

**Figure 11-17** Editing a Domain Menu



**Tip:** After you edit a menu, it is a good practice to change the mode to **only admins are allowed to edit** in the **Mode** dropdown list in the **Edit** tab. Although the **Edit menu** link is automatically removed from the menu if the registered user is not an administrator, users may accidentally edit the menu page.

5. Click **Save**.

### 11.8.3.3 Managing Domain Members

By default, all authorized wiki users can view and modify wiki pages in a domain. However, you can choose to specify the users who can access and manage wiki pages in a domain.

To manage domain members:

1. In the Administration mode, click **Domains**.

2. On the Domains page, click the **manage members** link of the domain for which you want to specify members.
3. From the **username** dropdown list, select the user whom you want to add as a domain member.
4. Click **Add**.

The new user's name displays in the **Members** section, as shown in [Figure 11–18](#).

Repeat step 3 and 4 if you want to add any other user as the domain member.

**Figure 11–18 Adding a Domain Member**

Manage the members of Seattle

Username:

Members

- monty ([remove](#))

5. Click the **remove** link next to a member's name under **Members** if you do not want that member to be able to manage the domain.

While creating a wiki page in the domain, users can select the **restricted to members of the domain** option if they want only domain members to be able to edit the wiki page.

**Figure 11–19 Restricting Access to Domain Members**

Edit Page

Mode:

- editable by everyone
- restricted to logged in users
- restricted to members of the domain**

#### 11.8.3.4 Managing Blog Authors

By default, blog entries can be added only by a wiki administrator or the person who owns the blog. For a personal blog, blog author is the person who owns that personal blog. In a domain (such as a blog associated with a WebCenter group space), blog author is the domain creator, which is usually a wiki administrator.

A wiki administrator or the blog owner can specify additional users who can add blog entries. For information about enabling or disabling additional blog authors, see the "Adding and Removing Additional Blog Authors" section in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

---

**Note:** If a user creates a domain, the user does not automatically become the blog author for the domain blog. The user must be specifically added as a blog author.

---

## 11.8.4 Changing the Theme

You can apply themes to change the look and feel of your wiki and blog server.

To change the default theme:

1. In the Administration mode, under **General**, click **Configuration**.
2. Select a theme from the **Theme** dropdown list.
3. Click **Save**.

**Figure 11–20** *Selecting a Theme*

The screenshot shows the 'Configuration' page with a dropdown menu open for the 'Theme' field. The dropdown lists several themes, with 'Wiki Default (wiki)' selected. Other themes include Deep Sea (deepsea), Sand (sand), Monochrome (monochrome), White (white), Tech Gray (tech\_gray), Bighorn (bighorn), Storm (storm), Olive (olive), WebCenter Theme (webcenter), Red (red), WebCenter Default (default), Blue (blue), Blue Sky (bluesky), Onyx (onyx), and Flatirons (flatirons).

| Name                       | Description                 |
|----------------------------|-----------------------------|
| Theme                      | Wiki Default (wiki)         |
| Max LRU                    | Deep Sea (deepsea)          |
| Default page encoding      | Sand (sand)                 |
| Default Domain             | Monochrome (monochrome)     |
| Max attachment size        | White (white)               |
| Supported attachment types | Tech Gray (tech_gray)       |
|                            | Bighorn (bighorn)           |
|                            | Storm (storm)               |
|                            | Olive (olive)               |
|                            | WebCenter Theme (webcenter) |
|                            | Red (red)                   |
|                            | WebCenter Default (default) |
|                            | Blue (blue)                 |
|                            | Blue Sky (bluesky)          |
|                            | Onyx (onyx)                 |
|                            | Wiki Default (wiki)         |
|                            | Flatirons (flatirons)       |

4. Click **Exit** to exit the Administration mode and see your changes take effect.

---

**Note:** Users can change the theme for a login session if they use a wiki or blog URL that includes the theme parameter.

---

## 11.8.5 Creating a User Interface Template

Templates enable you to set up a framework for users when they create pages. You can create new user interface templates as well as edit or delete existing ones.

To create a template:

1. In the Administration mode, under **General**, click **Templates**. The list of existing templates displays.

You can edit, view, or delete templates by clicking the appropriate link displayed in the **Actions** column, as shown in [Figure 11–21](#).

2. Click **add** to create a new template.

**Figure 11–21** *Managing Templates*

The screenshot shows the 'Templates' page with an 'add' link at the top. Below is a table listing existing templates and their actions.

| Name                 | Actions  |
|----------------------|--|
| SimpleHTMLPage       | <a href="#">edit</a><br><a href="#">delete</a><br><a href="#">view</a> |
| SimpleWikiMarkupPage | <a href="#">edit</a><br><a href="#">delete</a><br><a href="#">view</a> |

3. Enter the name of the template in the **Name** field in the **Add template** page.

While creating or editing a template, use the correct syntax. If the template is intended as a template for wiki markup, then use wiki markup. If it is intended to be a template for HTML pages, then use HTML. Template names should follow the same convention as page names.

4. Enter the content for the template in the **Template** box.
5. Click **Save**.

After you create a new template, users can choose to use this new template while creating a new page, as shown in [Figure 11–22](#).

**Figure 11–22** *Creating a Page Based on a Template*

The screenshot shows the 'New Wiki Page' form. At the top, it says 'Please provide a valid page name'. Below that is a 'Page name:' label and a text input field containing 'Seattle'. Underneath, it says 'Please select the type of page to create. If this is set to HTML, it cannot be changed to wiki markup after the page has been created.' There is a 'Type:' label and a dropdown menu currently set to 'HTML'. Below that, it says 'You can select a template here to create the page or decide to create an empty page'. There is a 'Template:' label and a dropdown menu. The dropdown menu is open, showing options: 'Create empty page', 'Create empty page', 'SimpleHTMLPage', 'SimpleWikiMarkupPage', and 'SimplePage'. A 'New' button is visible to the left of the dropdown menu.

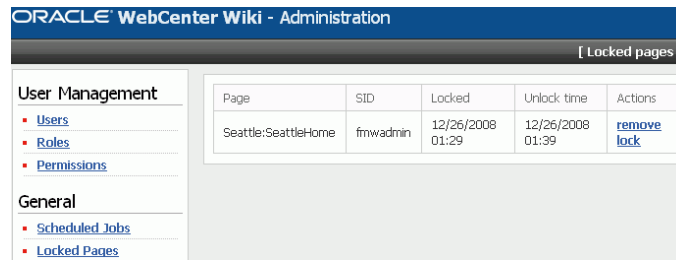
## 11.8.6 Unlocking a Page

Every time a user edits a wiki page, the page gets locked for a specified time period for that user before other users can modify that page. Sometimes an administrator may need to unlock a page. For example, if a user starts editing a wiki page and then clicks away from that page without clicking the Save or the Cancel button, then the page is still considered locked for editing. If another user tries to edit the same page, a warning message displays that the page is currently being edited by some other user, and any changes may be overwritten by a newer version. An administrator can unlock the page manually to remove this warning.

To unlock a page:

1. In the Administration mode, under **General**, click the **Locked Pages** link. A list of all the locked pages displays.
2. In the Locked pages page, click the **remove lock** link for the page you want to unlock. ([Figure 11–23](#))

**Figure 11–23 Unlocking a Page**



**Tip:** Details of a locked page are no longer displayed in Locked pages as soon as the page is unlocked, whether manually or automatically.

## 11.8.7 Setting Up Server Security

You can configure your wiki and blog server to leverage single sign-on security. You can use single sign-on options supported by Oracle WebCenter, such as Oracle Access Manager (OAM), Oracle Single Sign-On (OSSO), or a SAML-based single sign-on solution. For more information, see [Chapter 14, "Managing Security."](#)

When you integrate wikis and blogs into your applications, the users you set up for your applications must match the user created on the Oracle WebCenter Wiki and Blog Server. Once a user is authenticated, if the user does not exist within Oracle WebCenter Wiki and Blog Server, the user is created and a default role is assigned to the user.

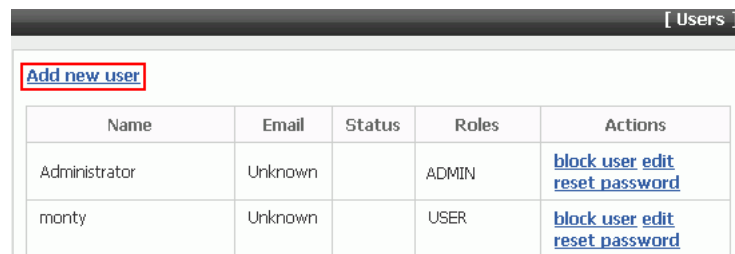
## 11.8.8 Managing Users and Roles

You can add users on the wiki and blog server and assign them required roles. You can also create new roles and assign the required permissions.

### 11.8.8.1 Managing Users

You can add a new user by using the **Add new user** link on the Users page in the Administration mode, as shown in [Figure 11–24](#). Adding users by this method adds users to the local security store of the wiki and blog server. This security store is used when there is no single sign-on security or an LDAP-based identity store configured for the wiki and blog server.

**Figure 11–24 Adding a User**



When you deploy the wiki and blog server by leveraging the single sign-on security, users are not initially imported from the external security store. Once a user is authenticated by the external security store, the wiki and blog server checks whether the user exists in its local security store. If not, a user entry is created upon first login by that user and a default role, like USER, is assigned to that user.



In the Administration mode, you can block users and reset passwords. These features are useful only when the wiki and blog server is used as a standalone application. Changing user passwords through the Administration mode changes passwords only in the local security store. If the server is integrated with another Oracle application through single sign-on or LDAP, then the user is authenticated through single sign-on and password are stored in the external security repository. In such a case, if a password needs to be changed, then you must change the password in the external security store.

### 11.8.8.2 Managing Permissions for a Role

For different wiki operations, you can create specific roles and assign required permissions to those roles. You can also modify existing roles to add or remove permissions. You can then assign the required roles to different users to define the operations that those users can perform.

To edit the permissions granted to a role:

1. In the Administration mode, under **User Management**, click **Roles**.

The Roles page displays various roles and the permissions assigned to each role.

2. Click the **edit** link under the role that you want to modify. For example, to modify the ADMIN role, you click **edit** under **ADMIN**. (Figure 11–25)

The Edit role page displays a list of all permissions that have been assigned or that can be assigned to the selected role. (Figure 11–26)

**Figure 11–25** Editing a Role

| ADMIN            |   |
|------------------|---|
| Name             | Permissions                                     |
| AttachFile       | User can attach files to a wiki page            |
| BlogAdmin        | User is allowed manage the authors of the Blogs |
| AdminTemplates   | User can edit and add templates                 |
| AdminPermissions | User can administer the set of permissions      |

**Tip:** If you want to create a new role, then specify a role name in the **Name** box and then click **Save** on the Roles page (Figure 11–25). You can then click the **edit** link under the newly created role to add the required permissions.

3. In the Actions column, click the **add** link for a permission to add that permission to the selected role, or click the **remove** link corresponding to a permission to remove that permission from the selected role. (Figure 11–26)

**Tip:** You can view the description of each permission by clicking **Permissions** under **User Management** on the navigation panel in the Administration mode.

**Figure 11–26 Specifying Permissions for a Role**

| [ Edit role ]      |         |                        |
|--------------------|---------|------------------------|
| <b>Role: ADMIN</b> |         |                        |
| Permissions        | Granted | Actions                |
| AdminDomains       | yes     | <a href="#">remove</a> |
| MailSetup          | yes     | <a href="#">remove</a> |
| ExportDomain       | no      | <a href="#">add</a>    |
| DeletePage         | yes     | <a href="#">remove</a> |
| AdminConfiguration | yes     | <a href="#">remove</a> |
| AdminTemplates     | yes     | <a href="#">remove</a> |
| Synchronize        | yes     | <a href="#">remove</a> |

4. Click the **Roles** link at the bottom of the Edit role page to return to the Roles page.

### 11.8.9 Enabling Anonymous Access

By default, only authenticated users can access your wiki and blog server. However, you can also enable anonymous access so that public users can view pages without logging in.

To enable anonymous access to your wiki and blog server:

1. In the Administration mode, under **General**, click **Settings**.
2. For the **Only logged in users can see the content** option, select **false** to allow anonymous read access. (Figure 11–27)
3. For **Anonymous users can create pages**, select **true** if you want to allow anonymous write access.

**Figure 11–27 Enabling Anonymous Access**

| Description                              | Value | Change                  |
|--|-------|-------------------------|
| Support friends                          | false | <a href="#">false</a> ▼ |
| Support self-registration of users       | true  | <a href="#">true</a> ▼  |
| Anonymous users can create pages         | false | <a href="#">false</a> ▼ |
| Support forum for every page             | false | <a href="#">false</a> ▼ |
| Support page ratings                     | false | <a href="#">false</a> ▼ |
| Support mail receiving for domains       | false | <a href="#">false</a> ▼ |
| Only logged in users can see the content | true  | <a href="#">true</a> ▼  |
| Support WYSIWYG editing                  | true  | <a href="#">true</a> ▼  |
| Allow users to delete pages they created | false | <a href="#">false</a> ▼ |
| Support trackbacks                       | false | <a href="#">false</a> ▼ |
| Support attachments                      | false | <a href="#">false</a> ▼ |
| Show the page menu                       | true  | <a href="#">true</a> ▼  |
| Support remote synchronization           | false | <a href="#">false</a> ▼ |
| Show page info                           | true  | <a href="#">true</a> ▼  |

4. Click **Save**.

## 11.8.10 Blocking an IP Address

You can block selected IP addresses from creating or updating wiki pages on your wiki and blog server. However, a blocked IP address can still access the server to view wiki pages.

To block an IP address:

1. In the Administration mode, under **General**, click **Blacklist**.
2. In the **IP** field, enter the IP address that you want to block.
3. Click **Add**.

The IP address that you block displays in the list of blocked IP addresses. (Figure 11–28)

**Figure 11–28** Blocking an IP Address

[ Blacklist ]

Add IP to blacklist

IP:

| IP             | Actions                |
|----------------|------------------------|
| 10.177.255.100 | <a href="#">delete</a> |

## 11.8.11 Deleting Wiki Pages and Blog Entries

As a wiki administrator, you can delete wiki pages and blog entries that are no longer required.

### 11.8.11.1 Deleting a Wiki Page

To delete a wiki page:

1. Access the Administration mode.
2. Under **Domain Related**, click **All Pages**. This displays a list of all pages in the current domain.

---

**Note:** To delete wiki pages of any domain, you must first navigate to that domain and then access the Administration mode.

---

3. For the wiki page that you want to delete, click the corresponding **delete** link in the **Actions** column, as shown in Figure 11–29. If you want to delete multiple pages, then select checkboxes for specified pages in the **Delete** column, and then click **Delete Selected**.

**Figure 11–29 Deleting a Wiki Page**

| Delete                              | Name                             | Revision | Mode                 | Last Update      | Last Author | Actions                                       |
|-------------------------------------|----------------------------------|----------|----------------------|------------------|-------------|---|
| <input checked="" type="checkbox"/> | <a href="#">CustomerTraining</a> | 1        | editable by everyone | 01/21/2009 02:50 | fmwadmin    | <a href="#">delete</a> <a href="#">reduce</a> |
| <input type="checkbox"/>            | <a href="#">Menu</a>             | 0        | editable by everyone | 01/21/2009 00:13 | fmwadmin    | <a href="#">delete</a> <a href="#">reduce</a> |
| <input type="checkbox"/>            | <a href="#">SeattleHome</a>      | 0        | editable by everyone | 01/21/2009 00:13 | fmwadmin    | <a href="#">delete</a> <a href="#">reduce</a> |

Delete Selected

- Click the **Delete all empty pages** link at the top on the All Pages page if you want to delete wiki pages that do not contain any text.

Click the **reduce** link to reduce the versions of a wiki page available on the server. It makes the current or the latest version of a wiki page as the only version and deletes all previous versions.

---

**Note:** Users can delete the wiki pages that they created only if you select **true** for the **Allow users to delete pages they created** option. You access this option by selecting **Settings** under **General** in the Administration mode. If this option is enabled, then a Delete icon is displayed on the wiki pages that users create.

If the option is set to **false**, then only administrators can delete wiki pages.

---

#### 11.8.11.2 Deleting a Blog Entry

A wiki administrator or users who have the permission to manage blogs can edit and delete blog entries. For information about how to delete blog entries, see the "Deleting a Blog Entry" section in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

### 11.8.12 Specifying Configuration Parameters

There are several settings that you can configure in the Administration mode of your wiki and blog server. These include:

- Setting the default theme of your server
- Setting the maximum number of LRU pages stored
- Specifying the default page encoding format
- Specifying the default domain of the server
- Specifying the maximum attachment size in kilobytes (KB) supported on the server
- Specifying the attachment types supported on the server
- Specifying the default wiki page of the server
- Specifying the wiki repository to be either a file-based repository or a database storage. For more information, see [Section 11.8.13, "Configuring Wiki Repository."](#)

You specify these settings on the Configuration page, which you can access by selecting **Configuration** under **General** in the Administration mode. [Figure 11-30](#) shows various settings that you can configure for your wiki and blog server.

**Figure 11-30 Configuration Page**

The screenshot shows the Configuration page with a table of settings. The table has two columns: Name and Description. The settings are as follows:

| Name                       | Description                 |
|----------------------------|-----------------------------|
| Theme                      | Wiki Default (default) ▼    |
| Max LRU                    | 10                          |
| Default page encoding      | UTF-8                       |
| Default Domain             | owc_wiki                    |
| Max attachment size        | 1024                        |
| Supported attachment types | gif,jpg,png,doc,xls,ppt,pdf |
| Default Wiki page          | owc_wiki>WelcomePage        |
| Repository                 | Database backend ▼          |

Below the table is a Save button.

### 11.8.13 Configuring Wiki Repository

By default, Oracle WebCenter Wiki and Blog Server uses a database-based repository for domains and wikis and blogs. Data for some wiki-related objects (like attachments, templates, and server configuration values) is stored on the file system in a file-based repository at the following location:

```
$WLS_HOME/user_projects/domains/owc_wiki/servers/wiki_server/stage/11.1.1.1.0/owc_wiki
```

Where, *\$WLS\_HOME* is the Oracle WebLogic Server installation directory, *owc\_wiki* refers to the wiki and blog server domain, *wiki\_server* refers to the server to which the wiki and blog application is deployed, and *owc\_wiki* refers to the wiki and blog server deployment directory.

You specify the wiki repository setting on the Configuration page in the Administration mode. You can switch to a file-based repository by selecting the **File based repository** option from the **Repository** list.

For file-based repository, the wiki and blog server uses an HSQL database. If you switch from a database repository to a file-based repository, then to start the HSQL database, you must restart the server to which your wiki and blog server is deployed.

HSQL database runs on a specific default port, 1475. If that port is not available, then after deploying the wiki and blog server, you can modify the port in both the `beans.xml` file and the `application_config.script` file. These files are located in the following directory:

```
$WLS_HOME/user_projects/domains/owc_wiki/servers/wiki_server/stage/11.1.1.1.0/owc_wiki/WEB-INF/classes
```

## 11.8.14 Specifying Features Supported on the Wiki and Blog Server

As an administrator, you can choose to enable or disable certain features on your wiki and blog server. For example, you can specify whether attachments, page menu, and remote synchronization are supported. [Figure 11–31](#) shows the list of features that you can configure.

To set your wiki and blog server features, in the Administration mode, click the **Settings** link, and then select the value for the specified features as **true** or **false**, as shown in [Figure 11–31](#).

**Figure 11–31 Wiki and Blog Server Settings**

| Description                              | Value | Change  |
|--|-------|---------|
| Support friends                          | false | false ▾ |
| Support self-registration of users       | true  | true ▾  |
| Anonymous users can create pages         | false | false ▾ |
| Support forum for every page             | false | false ▾ |
| Support page ratings                     | false | false ▾ |
| Support mail receiving for domains       | false | false ▾ |
| Only logged in users can see the content | true  | true ▾  |
| Support WYSIWYG editing                  | true  | true ▾  |
| Allow users to delete pages they created | false | false ▾ |
| Support trackbacks                       | false | false ▾ |
| Support attachments                      | false | false ▾ |
| Show the page menu                       | true  | true ▾  |
| Support remote synchronization           | false | false ▾ |
| Show page info                           | true  | true ▾  |

Save

## 11.8.15 Monitoring Oracle WebCenter Wiki and Blog Server

You can monitor your wiki and blog server by viewing the log file, `owc_wiki.log`. This file is located in the `$WLS_HOME/user_projects/domains/owc_wiki` directory, where `$WLS_HOME` is the directory where you installed Oracle WebLogic Server and `owc_wiki` is your wiki domain.

To change the log level, modify the `jlo_logging.xml` file located at the following path:

```
$WIKI_HOME/WEB-INF/classes
```

Where, `$WIKI_HOME` is the wiki and blog server deployment directory.

For example, the following is a sample path to the `jlo_logging.xml` file:

```
D:/Oracle/Middleware/user_projects/domains/owc_wiki/servers/wikiserver/stage/owc_wiki/owc_wiki/WEB-INF/classes
```

Where, `owc_wiki` is the wiki domain and `wikiserver` is the managed server on which the wiki and blog server is deployed.

You can change the targets of the loggers in this file. The following targets are supported currently: `trace`, `info`, `debug`, `warn`, `error`, and `fatal`. You can also use

two special targets: `off` (to switch off all the targets) or `all` (to switch on all the targets). For more information on the jLo logger, see <http://jlo.jzonic.org/GettingStarted.html>.

---

**Note:** You can also change the location of the log file using the jLo handlers. For more information, see <http://jlo.jzonic.org/AllHandlers.html>.

---

### 11.8.16 Backing Up and Restoring Wiki Content

By default, the wiki and blog server is configured to use a database repository. You can back up all your wiki content in the database by using SQL scripts or any database backup tool. If your wiki and blog server uses a file-based repository, you can back up your wiki content to a file system.

To back up the wiki content stored in a file-based repository:

1. Make a copy of the `$WIKI_HOME/pages` directory, where `$WIKI_HOME` refers to the wiki and blog server deployment directory.

For example, the following is a sample path where domain files may be stored:

```
D:/Oracle/Middleware/user_projects/domains/owc_
wiki/servers/wikiserver/stage/owc_wiki/owc_wiki/pages
```

Where, `owc_wiki` is the wiki domain and `wikiserver` is the managed server on which the wiki and blog server is deployed.

2. Make a copy of the file system database `yawikiDB.script` located at the `$WIKI_HOME/WEB-INF/classes`.

You can restore the content by overwriting the `pages` folder and the file system database `yawikiDB.script` with the backup copies.

## 11.9 Setting Up the RSS Service

The RSS service can expose external content and information from WebCenter services as news feeds in WebCenter applications. Depending on your network configuration, proxy details may be required to display content from external RSS news feeds.

Use the WLST commands `setRSSProxyConfig` to specify the proxy host and port for the RSS service. For command syntax and examples, see "setRSSProxyConfig" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands"](#).

---

**Note:** To start using new proxy details you must restart the managed server on which the WebCenter application is deployed. See, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

---

See also, "Chapter 18 Working with the RSS Service" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

### **Testing RSS News Feed Connections**

To ensure that the proxy information is accurately configured for the RSS News Feed service:

1. In WebCenter Spaces, drag and drop RSS Viewer to a page.
2. Edit the RSS Viewer task flow and set the URL to an external RSS feed. For example, `http://rss.cnn.com/rss/cnn_topstories.rss`. If this feed renders correctly, it confirms that the proxy configuration is set up properly.



---

---

## Managing Portlet Producers

This chapter describes how to register, edit, delete, and deploy portlet producers.

This chapter includes the following sections:

- [What You Should Know About Portlet Producers](#)
- [Registering WSRP Producers](#)
- [Testing WSRP Producer Connections](#)
- [Registering Oracle PDK-Java Producers](#)
- [Testing Oracle PDK-Java Producer Connections](#)
- [Editing Producer Registration Details](#)
- [Deregistering Producers](#)
- [Deploying Portlet Producer Applications](#)

### Audience

The content of this chapter is intended for Fusion Middleware administrators (users granted the `Admin` or `Operator` role through the Oracle WebLogic Server Administration Console). See also, [Section 1.8, "Understanding Administrative Operations, Roles, and Tools"](#).

## 12.1 What You Should Know About Portlet Producers

- Several out-of-the-box producers are provided with Oracle WebCenter: OmniPortlet, Web Clipping, Rich Text Portlet, and WSRP Tools.
  - `portalTools.ear` - OmniPortlet and Web Clipping
  - `wsrp-tools.ear` - Rich Text Portlets and WSRP Tools

The `portalTools.ear` and `wsrp-tools.ear` files are installed using the `registerOOTBProducers WLST` command. For command syntax and examples, see "registerOOTBProducers" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

- WSRP and Oracle PDK-Java producers are required to be registered. See also, "registerSampleProducers" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.
- The Oracle Portlet Producer product (server) must be installed in the production environment and the `wsrp-tools` and `portalTools` URLs must be accessible. If the Oracle Portlet Producer is not already installed, see the section "Extending an

Existing Domain" in the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter* to install it in the production environment.

- When a connection is created to a portlet producer, the producer gets registered with the WebCenter application and the connection is added to the `connections.xml` file during registration. For WSRP producers, a Web service connection is also created, which follows the naming convention, `connectionname-wsconn`. For Oracle PDK-Java producers, an underlying URL connection is created, which follows the naming convention, `connectionname-urlconn`. During the registration, the connection metadata is created in the MDS and in the producer being registered. When a producer is consumed, the user customizations are saved to the producer. During de-registration the producer connection and customizations are removed.
- All post deployment connection configuration is stored in Oracle Metadata Services (MDS) repository. See [Section 1.3.4, "Oracle WebCenter Configuration Considerations."](#) For detailed information about MDS, see the chapter "Managing the Oracle Metadata Repository" in the *Oracle Fusion Middleware Administrator's Guide*.
- Portlet producer registration is dynamic. New portlet producers and updates to existing producers are immediately available; there is no need to restart the WebCenter application or the managed server.
- To migrate producers from one instance to another, use the migration utilities described in the appendix "Portlet Preference Store Migration Utilities" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.
- For information on securing portlet producers, see [Section 14.8.4, "Securing a WSRP Producer with WS-Security"](#) and [Section 14.9, "Securing a PDK-Java Producer."](#)

## 12.2 Registering WSRP Producers

This section includes the following sub sections:

- [Registering a WSRP Producer Using Fusion Middleware Control](#)
- [Registering a WSRP Producer Using WLST](#)

### 12.2.1 Registering a WSRP Producer Using Fusion Middleware Control

To register a WSRP portlet producer:

1. Login to Fusion Middleware Control and navigate to the home page for your custom WebCenter application (or WebCenter Spaces):
  - [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#).
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)
2. Do one of the following:
  - For custom WebCenter applications - From the **Application Deployment** menu, choose **WebCenter > Register Producer**
  - For WebCenter Spaces - From the **WebCenter** menu, choose **Register Producer**.
3. In the **Add Portlet Producer Connection** section, enter connection details for the WSRP producer.

For detailed parameter information, see [Table 12–1, "WSRP Producer Connection Parameters"](#).

**Table 12–1 WSRP Producer Connection Parameters**

| Field           | Description   |
|-----------------|---|
| Connection Name | <p>Enter a unique name that will identify this portlet producer registration within the WebCenter application. The name must be unique across all WebCenter connection types.</p> <p>The name you specify here will appear in the Oracle Composer (under the <i>Portlets</i> folder).</p>   |
| Producer Type   | Indicate the type of this producer. Choose <b>WSRP Producer</b> .   |
| WSDL URL        | <p>The registration URL for the WSRP producer.</p> <p>The syntax will vary according to your WSRP implementation. For example, possible URL formats for a portlet deployed to the Oracle WSRP container include:</p> <pre>http://host_name:port_number/context_root/portlets/wsrp2?WSDL</pre> <pre>http://host_name:port_number/context_root/portlets/wsrp1?WSDL</pre> <pre>http://host_name:port_number/context_root/portlets/?WSDL (WSRP 1.0 for backward compatibility)</pre> <p>Where:</p> <ul style="list-style-type: none"> <li>■ <code>host_name</code> is the server where your producer is deployed</li> <li>■ <code>port_number</code> is the HTTP listener port number</li> <li>■ <code>context_root</code> is the Web application's context root</li> <li>■ <code>portlets_wsrp(1 2)?WSDL</code> is static text. All producers deployed to the Oracle WSRP container are exposed as WSRP version 1 and version 2 producers.</li> </ul> <p>In WebCenter Spaces, only v2 WSDLs are supported for Oracle WebLogic Portal Producers.</p> <p>For example:</p> <pre>http://myhost.com:7778/MyPortletApp/portlets/wsrp2?WSDL</pre> <p>For Oracle WSRP producers, this registration URL can be obtained by accessing the producer test page at:</p> <pre>http://host_name:port_number/context_root/info</pre> |
| Use Proxy?      | <p>Select if the WebCenter application must use an HTTP proxy when contacting this producer. If selected, enter values for <b>Proxy Host</b> and <b>Proxy Port</b>.</p> <p>A proxy is required when the WebCenter application and the remote portlet producer are separated by a firewall and an HTTP proxy is needed to communicate with the producer.</p>   |
| Proxy Host      | <p>Enter the address for the proxy server.</p> <p>Do not prefix <code>http://</code> to the proxy server name.</p>  |
| Proxy Port      | Enter the port number on which the proxy server listens. The default port is 80.  |

**Table 12–1 (Cont.) WSRP Producer Connection Parameters**

| Field                               | Description   |
|-------------------------------------|---|
| Default Execution Timeout (Seconds) | <p>Enter a suitable timeout for design-time operations. For example, the maximum time the producer may take to register, deregister, or display portlets on WebCenter pages.</p> <p>Individual portlets may define their own timeout period, which takes precedence over the value expressed here.</p> <p>This default is 30 seconds.</p> |

4. Use the **Security** section to specify the type of security token to use for the identity propagation/assertion.

The security token with the propagated or asserted user information is represented as an XML element in the SOAP header. The security token and the SOAP message body are then digitally signed to prove the authenticity of the SOAP message origin from the WebCenter application. WebCenter Spaces supports three types of security tokens: *Username Tokens Without Password*, *Username Tokens With Password*, and *SAML Tokens*.

---

**Note:** PeopleSoft WSRP producers support two profiles: *Username Token With Password* and *SAML Token With Message Integrity*. Oracle Portal (as a consumer) support three profiles: *Username Token Without Password*, *Username Token With Password*, *SAML Token With Message Integrity*. Other Oracle WSRP producers support all four profiles. For other WSRP containers, check with the specific vendor to determine the token formats they support.

---

For detailed parameter information, see [Table 12–2, "WSRP Producer Security Connection Parameters"](#).

**Table 12–2 WSRP Producer Security Connection Parameters**

| Field         | Description  |
|---------------|--|
| Token Profile | <p>Select the type of token profile to use for authentication with this WSRP producer. Choose from:</p> <ul style="list-style-type: none"> <li> <p>■ <b>Username Without Password</b><br/>           (oracle/wss10_username_id_propagation_with_msg_protection_client_policy)—Enforces message level protection (integrity and confidentiality) and identity propagation for inbound SOAP requests using mechanisms described in WS-Security 1.0. Message protection is provided using WS-Security 1.0's Basic128 suite of asymmetric key technologies. Specifically RSA key mechanisms for confidentiality, SHA-1 hashing algorithm for integrity and AES-128 bit encryption. Identity is set using a <i>username</i> provided through the UsernameToken WS-Security SOAP header. The subject is established against the currently configured identity store.</p> <p>When this policy is selected, the Recipient Alias must be specified.</p> </li> <li> <p>■ <b>Username With Password</b><br/>           (oracle/wss10_username_token_with_message_protection_client_policy)—Enforces message-level protection (message integrity and confidentiality) and authentication for inbound SOAP requests in accordance with the WS-Security v1.0 standard. It uses WS-Security's Basic 128 suite of asymmetric key technologies, specifically RSA key mechanism for message confidentiality, SHA-1 hashing algorithm for message integrity, and AES-128 bit encryption. Authentication is enforced using <i>credentials</i> in the WS-Security UsernameToken SOAP header. The subject is established against the currently configured identity store.</p> <p>Use this token profile if the WSRP producer has a different identity store. You will need to define an external application pertaining to the producer and associate the external application with this producer. External application defined here is used to retrieve and propagate the user credentials to the producer. The producer verifies this against the identity store configured for the external application.</p> <p>When this policy is selected, the Recipient Alias must be specified.</p> </li> <li> <p>■ <b>SAML Token With Message Integrity</b><br/>           (wss10_saml_token_with_message_integrity_client_policy)—Enforces message-level integrity protection and SAML-based authentication for inbound SOAP requests in accordance with the WS-Security 1.0 standard. It uses WS-Security's Basic 128 suite of asymmetric key technologies, specifically RSA key mechanisms for message confidentiality, SHA-1 hashing algorithm for message integrity.</p> </li> <li> <p>■ <b>SAML Token With Message Protection</b><br/>           (oracle/wss10_saml_token_with_message_protection_client_policy)—Enforces message-level protection and SAML-based authentication for inbound SOAP requests in accordance with the WS-Security 1.0 standard. It uses WS-Security's Basic 128 suite of asymmetric key technologies, specifically RSA key mechanisms for message confidentiality, SHA-1 hashing algorithm for message integrity, and AES-128 bit encryption.</p> <p>When this policy is selected, the Recipient Alias must be specified.</p> </li> <li> <p>■ <b>None</b>—No security on this connection. If None is selected, no WS-Security header is attached to the SOAP message.</p> </li> </ul> |

**Table 12–2 (Cont.) WSRP Producer Security Connection Parameters**

| Field  | Description   |
|--|---|
| Issuer Name  | <p>Enter the name of the issuer of the SAML Token.</p> <p>For example: <code>www.example.com</code></p> <p>The issuer name is the attesting entity that vouches for the verification of the subject, and it must be a trusted SAML issuer on the producer end.</p> <p>Valid for: SAML Token With Message Integrity and SAML Token With Message Protection</p>   |
| Default User   | <p>Enter a user name to assert to the remote producer when the user is not authenticated with the WebCenter application.</p> <p>When unauthenticated, the identity <i>anonymous</i> is associated with the application user. The value <i>anonymous</i> may be inappropriate for the remote producer, so you may need to specify an alternative identity here. Keep in mind though, that in this case, the WebCenter application has not authenticated the user so the default user you specify should be a low privileged user in the remote producer. If the user has authenticated to the application, the user's identity is asserted rather than the default user.</p> <p>The WSRP producer must be configured with <code>strict-authentication</code> to support <i>anonymous</i> to a default user mapping. The <code>strict-authentication</code> flag is defined in producer's <code>oracle-portlet.xml</code> file. For more information, see the appendix "oracle-portlet.xml Syntax" in <i>Oracle Fusion Middleware Developer's Guide for Oracle WebCenter</i>.</p> <p>Valid for: SAML Token With Message Integrity, SAML Token With Message Protection, and Username Without Password.</p> |
| Associated External Application (Username With Password) | <p>If this producer uses an external application for authentication, use the <b>Associated External Application</b> drop down list to identify the application. If application you want is not listed, select <b>Create New</b> to define the external application now.</p> <p>An external application is required to support producers using the security option <i>Username Token With Password</i>. The external application stores and supplies the user credentials. See also <a href="#">Section 13.2, "Registering External Applications."</a></p> <p>Valid for: Username With Password only.</p>  |

5. Use the **Keystore** section to specify the location of the key store that contains the certificate and private key that is used for signing some parts (security token and SOAP message body) of the SOAP message.

For detailed parameter information, see [Table 12–3, "WSRP Producer Key Store Connection Parameters"](#).

**Table 12–3 WSRP Producer Key Store Connection Parameters**

| Field      | Description  |
|------------|--|
| Store Type | The keystore type for this producer—always Java Key Store (jks).   |
| Store Path | <p>Enter the absolute path to the keystore that contains the certificate and the private key that is used for signing or encrypting the soap message (security token and message body). The signature, encryption, and recipient keys described in this table must be available in this keystore.</p> <p>The keystore should be created using JDK's keytool utility.</p> |

**Table 12–3 (Cont.) WSRP Producer Key Store Connection Parameters**

| Field                   | Description  |
|-------------------------|--|
| Password                | Provide the password to the keystore that was set when the keystore was created. The producer will not be available if a password is not specified or incorrect.     |
| Signature Key Alias     | Enter the signature key alias.<br><br>The <b>Signature Key Alias</b> is the identifier for the certificate associated with the private key that is used for signing. |
| Signature Key Password  | Enter the password for accessing the key identified by the alias specified in <b>Signature Key Alias</b> .   |
| Encryption Key Alias    | Enter the key alias to be used for encryption.   |
| Encryption Key Password | Enter the password for accessing the encryption key.   |
| Recipient Alias         | Specify the key store alias that is associated with the producer's certificate.<br><br>This certificate is used to encrypt the message to the producer.              |

6. Click **OK** to save WSRP producer details.

The new producer appears in the connection table.

The producer is now ready for consumption.

## 12.2.2 Registering a WSRP Producer Using WLST

Use the WLST command `registerWSRPProducer` to create a connection to a WSRP portlet producer and register the producer with your WebCenter application. For command syntax and examples, see "registerWSRPProducer" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

**See Also:** `deregisterWSRPProducer`, `listWSRPProducers`, `refreshProducer`, `registerOOTBProducers`, `registerSampleProducers`

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

## 12.3 Testing WSRP Producer Connections

To verify a WSRP producer connection, first obtain the producer URL from:

```
http://host_name:port_number/context_root/info
```

Then, run the producer URL to a browser window.

For a WSRP v1 producer connection, the URL format is:

```
http://host_name:port_number/context_root/portlets/wsrp1?WSDL
```

For example:

```
http://myhost.com:7778/MyPortletApp/portlets/wsrp1?WSDL
```

For a WSRP v2 producer connection, the URL format is:

```
http://host_name:port_number/context_root/portlets/wsrp2?WSDL
```

For example:

<http://myhost.com:7778/MyPortletApp/portlets/wsrp2?WSDL>

## 12.4 Registering Oracle PDK-Java Producers

This section includes the following sub sections:

- [Registering an Oracle PDK-Java Producer Using Fusion Middleware Control](#)
- [Registering an Oracle PDK-Java Producer Using WLST](#)

### 12.4.1 Registering an Oracle PDK-Java Producer Using Fusion Middleware Control

To register an Oracle PDK-Java portlet producer:

1. Login to Fusion Middleware Control and navigate to the home page for your custom WebCenter application (or WebCenter Spaces):
  - [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#)
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)
2. Do one of the following:
  - For custom WebCenter applications - From the **Application Deployment** menu, choose **WebCenter > Register Producer**.
  - For WebCenter Spaces - From the **WebCenter** menu, choose **Register Producer**.
3. In the **Add Portlet Producer Connection** section, enter connection details for the Oracle PDK-Java producer.

For detailed parameter information, see [Table 12-4, "Oracle PDK-Java Producer Connection Parameters"](#).

**Table 12-4 Oracle PDK-Java Producer Connection Parameters**

| Field           | Description  |
|-----------------|--|
| Connection Name | Enter a unique name that will identify this portlet producer registration within the WebCenter application. The name must be unique across all WebCenter connection types.<br><br>The name you specify here will appear in the Oracle Composer (under the <i>Portlets</i> folder). |
| Producer Type   | Indicate the type of this producer. Choose <b>Oracle PDK-Java Producer</b> .   |



**Table 12–4 (Cont.) Oracle PDK-Java Producer Connection Parameters**

| Field                           | Description  |
|---------------------------------|--|
| URL End Point                   | <p>Enter the Oracle PDK-Java producer's URL using the following syntax:</p> <pre>http://host_name:port_number/context_root/providers</pre> <p>Where:</p> <ul style="list-style-type: none"> <li>■ host_name is the server where the producer is deployed</li> <li>■ port_number is the HTTP Listener port number</li> <li>■ context_root is the Web application's context root.</li> <li>■ providers is static text.</li> </ul> <p>For example:</p> <pre>http://myHost.com:7778/myEnterprisePortlets/providers</pre>   |
| Service ID                      | <p>Enter a unique identifier for this producer.</p> <p>PDK-Java enables you to deploy multiple producers under a single adapter servlet. Producers are identified by their unique service ID. A service ID is required only if the service ID is not appended to the URL end point.</p> <p>For example, the following URL endpoint requires <code>sample</code> as the service ID:</p> <pre>http://domain.us.oracle.com:7778/xyz/providers</pre> <p>However, the following URL endpoint, does not require a service ID:</p> <pre>http://domain.us.oracle.com:7778/xyz/providers/sample</pre> <p>The service ID is used to look up a file called <code>&lt;service_id&gt;.properties</code>, which defines the characteristics of the producer, such as whether to display its test page. Use any value to create the service ID. When no Service ID is specified, <code>_default</code> is used.</p> |
| Use Proxy?                      | <p>Select this check box if the WebCenter application must use an HTTP proxy when contacting this producer. If selected, enter values for <b>Proxy Host</b> and <b>Proxy Port</b>.</p> <p>A proxy is required if the WebCenter application and the remote portlet producer are separated by a firewall and an HTTP proxy is needed for communication with the producer.</p>  |
| Proxy Host                      | <p>Enter the host name for the proxy server.</p> <p>Do not prefix <code>http://</code> to the proxy server name.</p>   |
| Proxy Port                      | <p>Enter the port number on which the proxy server listens. This argument defaults to 80.</p>  |
| Associated External Application | <p>If one of this producer's portlets requires authentication, select <b>Associate Producer with an External Application</b>, and then select the relevant external application from the drop-down list. See also <a href="#">Section 13.2, "Registering External Applications."</a></p>   |

**Table 12–4 (Cont.) Oracle PDK-Java Producer Connection Parameters**

| Field                               | Description   |
|-------------------------------------|---|
| Establish Session?                  | <p>Select to enable a user session when executing portlets from this producer. When sessions are enabled, they are maintained on the producer server. This allows the portlet code to maintain information in the session.</p> <p>Message authentication uses sessions, so if a shared key is specified, this option should also be selected.</p> <p>For sessionless communication between the producer and the server, do not select this option.</p>  |
| Default Execution Timeout (Seconds) | <p>Enter a suitable timeout for design-time operations. For example, the maximum time the producer may take to register, deregister, or display portlets on WebCenter pages. This defaults to 30 seconds.</p> <p>Individual portlets may define their own timeout period, which takes precedence over the value expressed here.</p>   |
| Subscriber ID                       | <p>Enter a string to identify the consumer of the producer being registered.</p> <p>When a producer is registered with an application, a call is made to the producer. During the call, the consumer (WebCenter application in this instance) passes the value for Subscriber ID to the producer. If the producer does not see the expected value for Subscriber ID, it might reject the registration call.</p>   |
| Shared Key                          | <p>Enter a shared key to use for producers that are set up to handle encryption.</p> <p>The shared key is used by the encryption algorithm to generate a message signature for message authentication. Note that producer registration will fail if the producer is set up with a shared key and you enter an incorrect shared key here. The shared key can contain between 10 and 20 alphanumeric characters.</p> <p>This key is also used when registering a producer using Federated Portal Adapter (FPA). The Shared Key is also known as the HMAC key.</p> |

4. Click **OK** to save Oracle PDK-Java producer details.

The new producer appears in the connection table.

## 12.4.2 Registering an Oracle PDK-Java Producer Using WLST

Use the WLST command `registerPDKJavaProducer` to create a connection to a PDK-Java portlet producer and register the producer with your WebCenter application. For command syntax and examples, see "registerPDKJavaProducer" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

**See Also:** `deregisterPDKJavaProducer`,  
`listPDKJavaProducers`, `refreshProducer`

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

## 12.5 Testing Oracle PDK-Java Producer Connections

To verify an Oracle PDK-Java producer connection, run the producer URL to a browser window in the following format:

```
http://host:port/context-root/providers/producer_name
```

For example:

```
http://domain.us.oracle.com:7778/xyz/providers/sample
```

## 12.6 Editing Producer Registration Details

You can update producer registration details at any time.

If a producer moves to a different location, then you must reconfigure any connections you have defined to this producer. You can use Fusion Middleware Control or WLST to edit the URL property:

- WDSL URL for a WSRP producer
- URL End Point for a Oracle PDK-Java producer

To retain all the portlet customizations and personalizations that users have made while working with WebCenter applications, you must migrate producer customizations and personalizations to the producer's new location, too. Use WLST commands `exportProducerMetadata` and `importProducerMetadata` to migrate portlet client metadata to a different location. See also, [Section 16.2.3, "Exporting Portlet Client Metadata \(Custom WebCenter Applications\)"](#) and [Section 16.2.4, "Importing Portlet Client Metadata \(Custom WebCenter Applications\)"](#).

---



---

**Note:** If you want to migrate all the metadata for a particular producer (rather than portlet customizations and personalizations only), then use the Producer migration tool. See also, [Section 16.1.3.13, "Exporting Portlet Producers"](#) and [Section 16.1.3.14, "Importing Portlet Producers."](#)

---



---

This section includes the following sub sections:

- [Editing Producer Registration Details Using Fusion Middleware Control](#)
- [Editing Producer Registration Details Using WLST](#)

### 12.6.1 Editing Producer Registration Details Using Fusion Middleware Control

To update connection details for a portlet producer:

1. Login to Fusion Middleware Control and navigate to the home page for your custom WebCenter application (or WebCenter Spaces):
  - [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#)
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)
2. Do one of the following:
  - For custom WebCenter applications - From the **Application Deployment** menu, choose **WebCenter > Service Configuration**.

- For WebCenter Spaces - From the **WebCenter** menu, choose **Settings > Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, choose **Portlet Producers**.
4. In the **Manage Portlet Producer Connections** section, select the producer you wish to modify, and click **Edit**.
5. In the **Edit Portlet Producer Connection** section, modify connection details, as required. For more information, see:
  - [Table 12–1, "WSRP Producer Connection Parameters"](#)
  - [Table 12–4, "Oracle PDK-Java Producer Connection Parameters"](#)
6. Click **OK** to save your changes.

## 12.6.2 Editing Producer Registration Details Using WLST

Use the following WLST commands to edit portlet producer connections:

- **WSRP producers** - `setWSRPProducer`
- **PDK-Java producers** - `setPDKJavaProducer`

For command syntax and examples, see the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

## 12.7 Deregistering Producers

You can deregister producers at any time but, before doing so, consider any impact to the WebCenter application as portlets associated with the producer will no longer work. Check the *Portlets Producer Invocation* metric to see how frequently the producer is being used. For more information, see [Section 15.2, "Viewing Performance Information."](#)

When you deregister a producer, registration data is removed from both the WebCenter application and the remote producer:

- WebCenter application - Producer connection is deleted and producer metadata is also deleted.
- Remote producer - Portlet instances are deleted (not the portlets themselves).

Portlet instances are not removed from WebCenter application pages. In place of the portlet, WebCenter users will see a "*Portlet unavailable*" message.

---

---

**Note:** Consider deleting the external application associated with this portlet producer *if* the application's sole purpose was to support this producer. See [Section 13.4, "Deleting External Application Connections."](#)

---

---

This section includes the following sub sections:

- [Deregistering Producers Using Fusion Middleware Control](#)
- [Deregister Producers Using WLST](#)

## 12.7.1 Deregistering Producers Using Fusion Middleware Control

To deregister a portlet producer:

1. Login to Fusion Middleware Control and navigate to the home page for your custom WebCenter application (or WebCenter Spaces):
  - [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#)
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)
2. Do one of the following:
  - For custom WebCenter applications - From the **Application Deployment** menu, choose **WebCenter > Service Configuration**.
  - For WebCenter Spaces - From the **WebCenter** menu, choose **Settings > Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, choose **Portlet Producers**.
4. Select the name of the producer you wish to remove, and click **Delete**.

The connection details are removed. Portlets associated with this producer are no longer accessible within the WebCenter application.

## 12.7.2 Deregister Producers Using WLST

Use the following WLST commands to deregister portlet producer connections:

- **WSRP producers** - `deregisterWSRPProducer`
- **PDK-Java producers** - `deregisterPDKJavaProducer`

Use the following WLST commands to deregister out-of-the-box or sample producers provided with Oracle WebCenter:

- **Out-of-the-box producers** - `deregisterOOTBProducers`
- **Sample producers** - `deregisterSampleProducers`

For command syntax and examples, see the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

## 12.8 Deploying Portlet Producer Applications

To deploy a portlet producer to an Oracle WebLogic Managed Server instance, you can use Fusion Middleware Control, Oracle WebLogic Server Administration Console, and WLST. For information on deploying portlet producer through Oracle JDeveloper, see the chapter "Testing and Deploying Your Portlets" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

This section includes the following subsections:

- [Understanding Portlet Producer Application Deployment](#)
- [Converting a JSR 168 Portlet Producer EAR File into a WSRP EAR File](#)
- [Deploying Portlet Producer Applications Using Oracle JDeveloper](#)
- [Deploying Portlet Producer Applications Using Fusion Middleware Control](#)

- [Deploying Portlet Producer Applications Using Oracle WebLogic Server Administration Console](#)
- [Deploying Portlet Applications Using WLST](#)

For more information about deploying applications, see the chapter "Deploying Application" in *Oracle Fusion Middleware Administrator's Guide*.

## 12.8.1 Understanding Portlet Producer Application Deployment

You can deploy your portlet producer application to any Oracle WebLogic Managed Server instance, which is configured to support WebCenter portlet producers. To deploy an application to a managed server, you can use Oracle Enterprise Manager Fusion Middleware Control, Oracle WebLogic Administration Console, and WLST. For more information about these administration tools, see [Section 1.12, "Oracle WebCenter Administration Tools."](#)

## 12.8.2 Converting a JSR 168 Portlet Producer EAR File into a WSRP EAR File

To deploy JSR 168 portlets to the WSRP Oracle Portlet Container, the portlet application EAR files must be converted into a WSRP application, which contains the necessary WSDL documents. To convert the JSR 168 portlet producer EAR file into a WSRP EAR file, run the WSRP producer predeployment tool located in the Middleware directory at `MW_HOME/WC_HOME/webcenter/modules/oracle.portlet.server_11.1.1.1`, as follows:

```
java -jar wsrp-predeploy.jar source EAR target EAR
```

For JPS-compliant portlets developed with servlet version 2.3, you must specify Web proxies using the following command:

```
java -Dhttp.proxyHost=proxy host -Dhttp.proxyPort=proxy port -jar wsrp-predeploy.jar source EAR target EAR
```

where:

`proxy host` is the server to which your producer has been deployed.

`proxy port` is the HTTP Listener port.

`wsrp-predeploy.jar` is located in the `MW_HOME/webcenter_home/modules/oracle.portlet.server_11.1.1.1` directory.

`source EAR` is the name of the JSR 168 EAR file.

`target EAR` file is the name of the new EAR file to be created. If the file name for the targeted EAR file is not specified, then a new EAR file called `WSRP-source EAR` is produced.

In the following example Web proxy is specified:

```
java -Dhttp.proxyHost=myhttpproxy.com -Dhttp.proxyPort=80 -jar wsrp-predeploy.jar wsrp-samples.ear
```

This example produces `WSRP-wsrp-samples.ear`.

The `wsrp-predeploy.jar` predeployment tool makes all the necessary changes to a JSR-168 portlet to be able to deploy it to the Oracle portlet container and expose it as a WSRP producer. Here are some examples of what the predeployment tool does:

- Creates the `wSDLdeploy` directory in the `java.io.tmpdir` folder.
  - On UNIX, the default value of this property is `/tmp` or `/var/tmp`

- on Microsoft Windows, the default value of this property is `c:\temp`.
- Unpacks the EAR file into `wsdldeploy/EAR`.
- Unpacks the WAR files into `wsdldeploy/[warfilename.war]/`.
- Inserts `WEB-INF/WSDLs` into the unpacked application.
- Modifies `WEB-INF/web.xml` in the unpackaged WAR files.
- Inserts or modifies `WEB-INF/webservices.xml` in the WAR files.
- Inserts or modifies `WEB-INF/oracle-webservices.xml` in the WAR files.
- Repackages the WARs and builds a new EAR file.

### 12.8.3 Deploying Portlet Producer Applications Using Oracle JDeveloper

You can deploy portlet applications to an Oracle WebLogic Managed Server instance directly from the development environment using Oracle JDeveloper, provided that you have the necessary credentials to access the WebLogic server. For more information, see the section "Deploying a Portlet Application to an Oracle WebLogic Managed Server Instance" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

### 12.8.4 Deploying Portlet Producer Applications Using Fusion Middleware Control

For information about deploying a portlet producer application using Fusion Middleware Control, see [Section 7.1.5.2, "Deploying Custom WebCenter Applications Using Fusion Middleware Control."](#)

### 12.8.5 Deploying Portlet Producer Applications Using Oracle WebLogic Server Administration Console

For information about deploying a portlet producer application using Oracle WebLogic Server Administration Console, see [Section 7.1.5.4, "Deploying WebCenter Applications Using the WLS Administration Console."](#)

### 12.8.6 Deploying Portlet Applications Using WLST

For information on deploying a portlet application using the WLST command, see [Section 7.1.5.3, "Deploying Custom WebCenter Applications Using WLST."](#)





---

---

## Managing External Applications

An external application is any application that implements its own authentication process. Specifically, it is an application that does not take part in your WebCenter application's single sign-on process.

You can use Fusion Middleware Control or the WLST command-line tool to register and manage external applications for WebCenter application deployments. All external application changes that you make for WebCenter applications, post deployment, are stored in the MDS repository as customizations.

---

---

**Note:** External application configuration through Fusion Middleware Control or WLST is dynamic. Configuration changes are immediately reflected in the WebCenter application; it is not necessary to restart the application or the managed server.

---

---

This chapter includes the following sections:

- [What You Should Know About External Applications](#)
- [Registering External Applications](#)
- [Modifying External Application Connection Details](#)
- [Deleting External Application Connections](#)

### **Audience**

The content of this chapter is intended for Fusion Middleware administrators (users granted the `Admin` or `Operator` role through the Oracle WebLogic Server Administration Console). See also, [Section 1.8, "Understanding Administrative Operations, Roles, and Tools."](#)

## 13.1 What You Should Know About External Applications

If your WebCenter application interacts with an application that handles its own authentication, you can associate that application with an external application definition to allow for credential provisioning. In doing so, you use an external application definition to provide a means of accessing content from these independently authenticated applications.

To replicate a single sign-on experience from the end user's perspective, the external application service captures the username and password, and any other credentials for the external application, and supplies it to the WebCenter service or application requiring the credentials. The WebCenter service or other application then uses this information to log in on behalf of the end user. This username and password

combination is securely stored in a credential store configured for the WebLogic domain where the application is deployed.

The user provides login credentials when prompted, and these credentials are mapped to the WebCenter application user and stored in the credential store configured for the domain. The credential store subsequently supplies that information during authentication to the external application. Unless the external application's credentials change, the user supplies the credentials only once as the mapped information is read from the credential store for future requests.

The external applications that are to be used by a custom WebCenter application can be specified before deployment through a wizard in Oracle JDeveloper, or after deployment through Fusion Middleware Control Console (Figure 13-1) or using WLST commands.

**Figure 13-1 Edit External Application**

## 13.2 Registering External Applications

You can register external applications for WebCenter applications through Fusion Middleware Control or using WLST commands.

Before registering an external application, access the application's login page and examine the HTML source for the application's login form. All the registration details you require are located in the `<form tag>`.

For example, the underlying code for the *Yahoo! Mail* login form looks something like this:

```
<form method=post action="https://login.yahoo.com/config/login?" autocomplete=off
name=login_form>
...
<td><input name=login size=17</td>
...
<td><input name=passwd size=17</td>
```

...

In this example, to provide WebCenter users with a direct link to the *Yahoo! Mail* application, the following sample registration information is required:

| Registration Information  | Sample Value                                | HTML Source              |
|---------------------------|---|--------------------------|
| Login URL                 | <code>https://login.yahoo.com/config</code> | <code>action</code>      |
|                           | <code>/login?</code>                        |                          |
| User Name / User ID Field | <code>login</code>                          | <code>name=login</code>  |
| Password Field Name:      | <code>passwd</code>                         | <code>name=passwd</code> |
| Authentication Method     | <code>post</code>                           | <code>method</code>      |

---

**Note:** External application configuration is dynamic. New external applications and updates to existing applications are immediately available; there is no need to restart the WebCenter application.

---

This section includes the steps for:

- [Registering External Applications Using Fusion Middleware Control](#)
- [Registering External Applications Using WLST](#)

### 13.2.1 Registering External Applications Using Fusion Middleware Control




To register an external application:

1. Login to Fusion Middleware Control and navigate to the home page for your WebCenter application (or WebCenter Spaces):
  - [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#).
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)
2. Do one of the following:
  - For custom WebCenter applications: from the **Application Deployment** menu, choose **WebCenter > Service Configuration**.
  - For WebCenter Spaces: from the **WebCenter** menu, choose **Settings > Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, choose **External Applications**.
4. To register a new external application, click **Add** ([Figure 13–2](#)).

**Figure 13–2 Configuring External Application Connections**

**Manage External Application Connections**

---

 Add
  Edit
  Delete

| Application Name | Display Name | Authentication Method |
|------------------|--------------|-----------------------|
| test             | Payroll      | POST                  |

5. Enter a unique name for the external application and a display name that WebCenter users working with this external application will see.

See also, [Table 13–1](#).

**Table 13–1 External Application Connection - Name**

| Field            | Description   |
|------------------|---|
| Application Name | Enter a name for the application. The name must be unique (across all connection types) within the WebCenter application.<br>For example: yahoo<br><b>Note:</b> Once registered, you cannot edit the Application Name.  |
| Display Name     | Enter a user friendly name for the application that WebCenter users will recognize. WebCenter end-users working with this external application will see the display name you specify here.<br>For example: My Yahoo<br>If you leave this field blank, the Application Name is used. |

6. Enter login details for the external application.

For details, see [Table 13–2](#).

**Table 13–2 External Application Connection - Login Details**

| Field                  | Description   |
|------------------------|---|
| Enable Automatic Login | Select to allow automatically log users in to this application. Choosing this option requires you to complete the Login URL, HTML User ID Field Name, and HTML User Password Field Name fields<br>With automated single sign-on, the user directly links to the application and is authenticated automatically, as their credentials are retrieved from the credential store. Selecting this option provides the end user with a seamless single sign-on experience.<br><b>Note:</b> Automated login is not supported for external applications using BASIC authentication. Automated login is also not supported for external sites that do not support UTF8 encoding. |

**Table 13–2 (Cont.) External Application Connection - Login Details**

| Field                         | Description   |
|-------------------------------|---|
| Login URL                     | <p>Enter the login URL for the external application.</p> <p>To determine the URL, navigate to the application's login page and record the URL.</p> <p>For example: <code>http://login.yahoo.com/config/login</code></p> <p><b>Note:</b> A login URL is not required if the sole purpose of this external application is to store and supply user credentials on behalf of another service. When omitted, the external application is not available for display in the <b>WebCenter Spaces</b> Application pane. See <a href="#">Section 21.2, "Making an Application Available to WebCenter Users."</a></p> |
| HTML User ID Field Name       | <p>Enter the name that identifies the "user name" or "user ID" field on the login form.</p> <p><b>Tip:</b> To find this name, look at the HTML source for the login page.</p> <p>This property does not specify user credentials.</p> <p><b>Note:</b> You must complete this field if the Authentication Method is GET or POST. Leave this field blank if the application uses basic authentication (see <b>Authentication Method</b>).</p>   |
| HTML User Password Field Name | <p>Enter the name that identifies the "password" field on the login form.</p> <p><b>Tip:</b> To find this name, look at the HTML source for the login page.</p> <p><b>Note:</b> You must complete this field if the Authentication Method is GET or POST. Leave this field blank if the application uses basic authentication (see <b>Authentication Method</b>).</p>   |

7. Select the authentication method used by the external application.

For details, see [Table 13–3](#).

**Table 13–3 External Application Connection - Authentication Details**

| Field                 | Description   |
|-----------------------|---|
| Authentication Method | <p>Select the form submission method used by the external application. Choose from one of the following:</p> <ul style="list-style-type: none"> <li>■ <b>GET:</b> Presents a page request to a server, submitting the login credentials as part of the login URL. This authentication method may pose a security risk because the user name and password are exposed in the URL.</li> <li>■ <b>POST:</b> Submits login credentials within the body of the form. This is the default.</li> <li>■ <b>BASIC:</b> Submits login credentials to the server as an authentication header in the request. This authentication method may pose a security risk because the credentials can be intercepted easily and this scheme also provides no protection for the information passed back from the server. The assumption is that the connection between the client and server computers is secure and can be trusted.</li> </ul> <p>The <b>Authentication Method</b> specifies how message data is sent by the browser. You can find this value by viewing the HTML source for the external application's login form, for example, <code>&lt;form method="POST" action="https://login.yahoo.com/config/login?AutoComplete="off"&gt;</code></p> |

8. Specify additional login fields and details, if required.

For details, see [Table 13–4, "External Application Connection - Additional Login Fields"](#).

**Table 13–4 External Application Connection - Additional Login Fields**

| Field                   | Description  |
|-------------------------|--|
| Additional Login Fields | <p>If your application requires additional login criteria, expand <b>Additional Login Fields</b>.</p> <p>For example, in addition to <i>user name</i> and <i>password</i>, the Lotus Notes application requires two additional fields - <i>Host</i> and <i>MailFilename</i>.</p> <p>Click <b>Add</b> to specify an additional field for the login form. For each new field, do the following:</p> <ul style="list-style-type: none"> <li>■ <b>Name</b> - Enter the name that identifies the field on the HTML login form that may require user input to log in. This field is not applicable if the application uses basic authentication.</li> <li>■ <b>Value</b> - Enter a default value for the field or leave blank for a user to specify. This field is not applicable if the application uses basic authentication.</li> <li>■ <b>Display to User</b> - Select to display the field on the external application login screen. If the field is not displayed (unchecked), then a default <b>Value</b> must be specified.</li> </ul> <p>Click <b>Delete</b> to remove a login field.</p> |

9. Specify shared and public user credentials, if required.

For details, see [Table 13–5](#).

**Table 13–5 External Application Connection - Shared User and Public User Credentials**

| Field                     | Description   |
|---------------------------|---|
| Enable Shared Credentials | <p>Indicate whether this external application enables shared user credentials, and specify the credentials. Select <b>Enable Shared Credentials</b>, and then enter <b>User Name</b> and <b>Password</b> credentials for the shared user.</p> <p>When shared credentials are specified, every user accessing this external application, through the WebCenter application, is authenticated using the user name and password defined here. WebCenter users are not presented with a login form.</p> <p>Because WebCenter users do not need to define personal credentials of their own, external applications with shared credentials are not listed in the external application's change password task flows such as <i>My Accounts</i> (see also <i>User's Guide -Managing Your Application Login Credentials</i>).</p> |
| Enable Public Credentials | <p>Indicate whether unauthenticated users (public users) may access this external application. Select <b>Enable Public Credentials</b>, and then enter <b>User Name</b> and <b>Password</b> credentials for the public user.</p> <p>When public credentials are specified, public users accessing this external application through the WebCenter application's public pages are logged in using the username and password defined here. If public credentials are not specified, public users will see an authorization error indicating this external application is not accessible to public users.</p>  |

10. Click **OK** to register the application.

In WebCenter Spaces, registered applications for automated login are not available to WebCenter users immediately. The WebCenter Spaces administrator decides which registered applications to expose through the Applications pane, see [Section 21.2, "Making an Application Available to WebCenter Users."](#)

### 13.2.2 Registering External Applications Using WLST

Use the WLST command `createExtAppConnection` to create an external application connection. For command syntax and examples, see `createExtAppConnection` in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

Use the WLST command `addExtAppCredentials` to add shared or public credentials for an existing external application connection. For details, see `addExtAppCredentials` in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

Use the WLST command `addExtAppField` to define additional login criteria for an existing external application connection. For details, see `addExtAppField` in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

## 13.3 Modifying External Application Connection Details

This section shows you how to modify the external application connection details by:

- [Modifying External Application Connection Using Fusion Middleware Control](#)

- [Modifying External Application Connection Using WLST](#)

### 13.3.1 Modifying External Application Connection Using Fusion Middleware Control

To update external application connection details:

1. Log in to Fusion Middleware Control and navigate to the home page for your custom WebCenter application (or WebCenter Spaces):
  - [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#).
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)
2. Do one of the following:
  - For custom WebCenter applications - from the **Application Deployment** menu, choose **WebCenter > Service Configuration**.
  - For WebCenter Spaces - from the **WebCenter** menu, choose **Settings > Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, choose **External Applications**.
4. Select the name of the external application you want to modify, and click **Edit**.
5. Edit connection details, as required. For detailed parameter information, see [Table 13–2](#).

Note that you cannot edit the name of the external application.
6. Click **OK** to save your changes.

### 13.3.2 Modifying External Application Connection Using WLST

Use the WLST command `setExtAppConnection` to edit existing external application connection details. For command syntax and examples, see `setExtAppConnection` in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

---

---

**Note:** To edit details relating to an additional login field, use `setExtAppField`. To edit existing shared or public credentials, use `setExtAppCredential`.

To delete an additional login field, use `removeExtAppField`. To delete shared or public credentials, use `removeExtAppCredential`.

---

---

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands"](#).

## 13.4 Deleting External Application Connections

Take care when deleting an external application connection as WebCenter application users will no longer have access to that application, and any services dependent on the external application may not function correctly.

In WebCenter Spaces, links to external applications are not automatically removed from the Applications pane when an external application is deleted. To prevent unsuccessful access attempts, administrators are advised to remove links to



unavailable applications. For details, see [Section 21.6, "Removing Links from the Applications Pane."](#)

This section includes the following subsections:

- [Deleting External Application Connections Using Fusion Middleware Control](#)
- [Deleting External Application Connections Using WLST](#)

### 13.4.1 Deleting External Application Connections Using Fusion Middleware Control

To delete an external application connection:

1. Login to Fusion Middleware Control and navigate to the home page for your WebCenter application (or WebCenter Spaces):
  - [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#).
  - [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#)
2. Do one of the following:
  - For WebCenter applications - from the **Application Deployment** menu, choose **WebCenter > Service Configuration**.
  - For WebCenter Spaces - from the **WebCenter** menu, choose **Settings > Service Configuration**.
3. From the list of services on the WebCenter Service Configuration page, choose **External Applications**.
4. Select the name of the external application you want to remove, and click **Delete**.

### 13.4.2 Deleting External Application Connections Using WLST

Use the WLST command `deleteConnection` to remove an external application connection. For command syntax and examples, see `deleteConnection` in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

---

---

**Note:** To delete an additional login field, use `removeExtAppField`.  
To delete shared or public credentials, use `removeExtAppCredential`.

---

---

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)



# Part IV

---

## Advanced Systems Administration for Oracle WebCenter

Part IV contains the following chapters:

- [Chapter 14, "Managing Security"](#)
- [Chapter 15, "Monitoring Oracle WebCenter Performance"](#)
- [Chapter 16, "Managing Export, Import, Backup, and Recovery of WebCenter"](#)



---

---

## Managing Security

This chapter describes how to configure your WebCenter application to handle authentication and authorization, and other aspects of application security.

This chapter includes the following sections:

- [Section 14.1, "Introduction to WebCenter Application Security"](#)
- [Section 14.2, "Default Security Configuration"](#)
- [Section 14.3, "Configuring the Identity Store"](#)
- [Section 14.4, "Configuring the Policy and Credential Store to Use OID"](#)
- [Section 14.5, "Managing Users and Roles"](#)
- [Section 14.6, "Configuring WebCenter Applications and Components to Use SSL"](#)
- [Section 14.7, "Configuring a WebCenter Application to Use Single Sign-On"](#)
- [Section 14.8, "Configuring WS-Security"](#)
- [Section 14.9, "Securing a PDK-Java Producer"](#)

### Audience

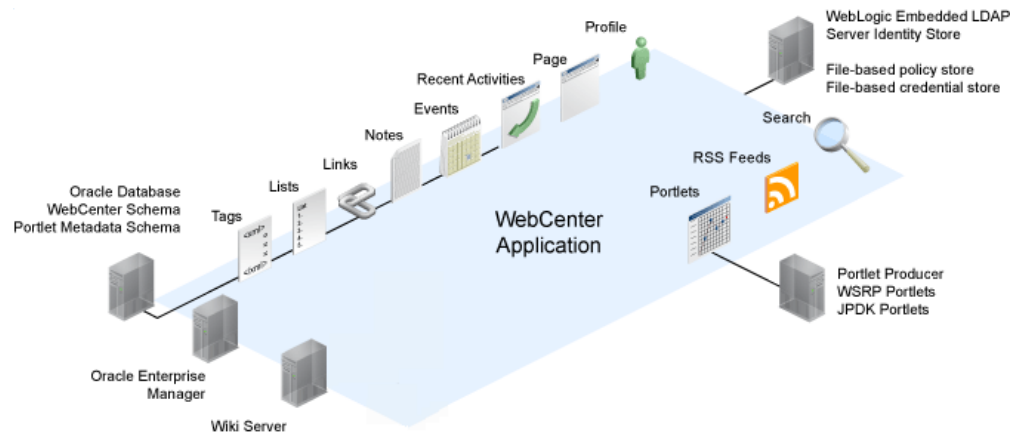
The content of this chapter is intended for Fusion Middleware administrators (users granted the `Admin` role through the Oracle WebLogic Server Administration Console). Users with the `Monitor` or `Operator` roles can view security information but cannot make changes. See also, [Section 1.8, "Understanding Administrative Operations, Roles, and Tools"](#).

## 14.1 Introduction to WebCenter Application Security

The recommended security model for Oracle WebCenter is based on Oracle ADF Security, which implements the Java Authentication and Authorization Service (JAAS) model. For more information about Oracle ADF Security, see the *Oracle Fusion Middleware Fusion Developer's Guide for Oracle Application Development Framework*.

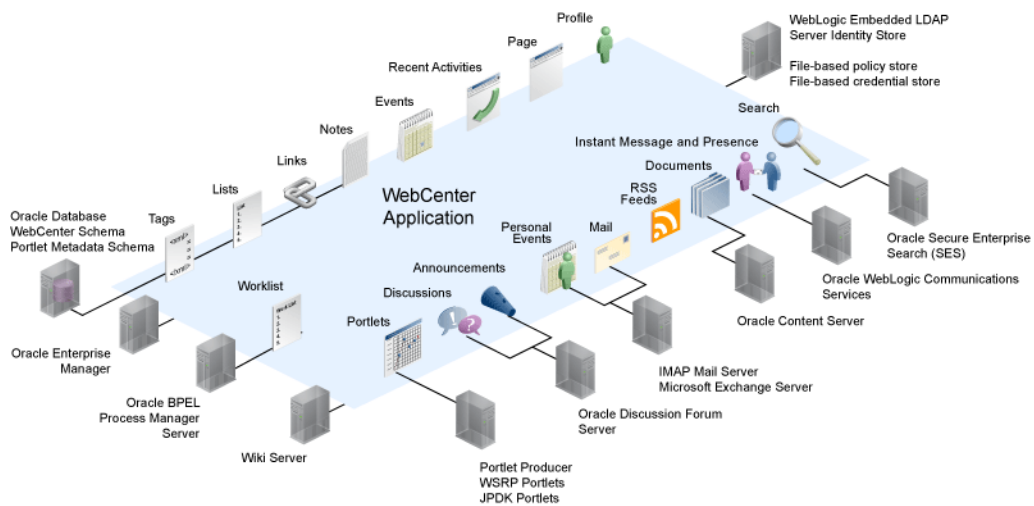
[Figure 14-1](#) shows the relationship between a WebCenter application deployment and its services, servers, portlets, portlet producers, its identity, credential and policy stores, and Oracle Enterprise Manager.

**Figure 14–1 Basic WebCenter Application Architecture**



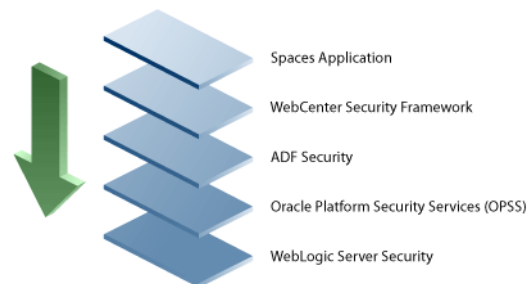
The diagram in [Figure 14–2](#) shows a basic WebCenter application after deployment with its back-end server connections.

**Figure 14–2 WebCenter Application Architecture with Back-end Server Connections**



The diagram in [Figure 14–3](#) shows the security layers for the WebCenter Spaces application.

**Figure 14–3 WebCenter Spaces Security Layers**



The security layers for a WebCenter application could have the same four bottom layers (WebCenter Security Framework, ADF Security, OPSS, and WebLogic Server Security) depending on how the application was structured. The application layer will, of course, depend on the implementation.

### **WebCenter Spaces Application Security**

WebCenter Spaces provides support for:

- Application role management and privilege mapping
- Self-registration
- Group space security management
- Account management
- External application credential management

### **WebCenter Security Framework**

WebCenter Security Framework provides support for:

- Service Security Extension Framework
- Permission-based authorization
- Role-mapping based authorization
- External applications and credential mapping

### **ADF Security**

ADF Security provides support for:

- Page authorization
- Task flow authorization
- Secure connection management
- Credential mapping APIs
- Logout invocation, including logout from SSO enabled configurations with Oracle Access Manager and Oracle SSO
- Secured login URL for ADF Security-based applications (the `adfAuthentication` servlet)

### **Oracle Platform Security Services (OPSS)**

OPSS provides support for:

- Anonymous-role support
- Authenticated-role support
- Identity store, policy store, and credential store
- Identity Management Services
- Oracle Web Service Manager Security

### **WebLogic Server Security**

WebLogic Server Security provides support for:

- WebLogic authenticators
- Identity asserters

- J2EE container security
- SSL

## 14.2 Default Security Configuration

This section describes the security configuration that is in place when custom WebCenter applications and WebCenter Spaces are deployed, and the tasks that need to be carried out after deployment:

- [Administrator Accounts](#)
- [Application Roles and Enterprise Roles in WebCenter Spaces](#)
- [Default Identity and Policy Stores](#)
- [Default Policy Store Permissions and Grants](#)
- [Post-deployment Security Configuration Tasks](#)

### 14.2.1 Administrator Accounts

Custom WebCenter applications do not contribute any pre-seeded accounts, and therefore rely on the administrator account (`weblogic` by default) that is set up when Fusion Middleware is installed. Use this administrator account to log into Fusion Middleware Control and set up new accounts.

Although WebCenter Spaces does not contribute any pre-seeded accounts, there are certain pre-seeded grants that are given to the default administrator account (`weblogic`) for the WebCenter Spaces application. If your installation does not use `weblogic` as the account name for the administrator role, you will need to configure one or more other users for this role as described in [Section 14.3.5.1, "Granting the WebCenter Spaces Administrator Role Using Fusion Middleware Control"](#).

### 14.2.2 Application Roles and Enterprise Roles in WebCenter Spaces

Application roles and permissions are defined within WebCenter Spaces and are stored in an application-specific stripe of the policy store. Consequently, WebCenter Spaces roles apply only to WebCenter Spaces; WebCenter Spaces roles and permissions do not extend to other applications.

Application roles differ from roles that appear in the identity store portion of the embedded LDAP server or in roles defined by the enterprise LDAP provider. Application roles are specific to an application and defined in the application policy store.

Enterprise roles, which are stored in the enterprise identity store, apply at the enterprise level. That is, the roles and permissions that you or a system administrator define within the enterprise identity store do not imply permissions within WebCenter Spaces.

Within WebCenter Spaces you can add users defined in the corporate identity store and assign them roles and permissions. You can also add roles defined in the enterprise identity store and assign permissions to those roles for WebCenter Spaces.



---

---

**Note:** When Groups (enterprise roles) are assigned to a group space role in WebCenter Spaces, the users that belong to that group (rather than the enterprise role) are added individually to the group space role. Consequently, be careful not to add groups with inordinately large amounts of users as performance during authentication may be affected.

---

---

### 14.2.3 Default Identity and Policy Stores

By default, WebCenter applications are configured to use a file-based embedded LDAP identity store to store application-level user IDs, and a file-based LDAP policy store to store policy grants.

Although secure, the embedded LDAP identity store is not a "production-class" store and should be replaced with an external LDAP-based identity store such as Oracle Internet Directory for enterprise production environments.

The default file-based policy store can only be used for single-node WebCenter Spaces configurations. For multi-node configurations, you must reassociate the policy and credential store with an external LDAP-based store (such as Oracle Internet Directory) as described in [Section 14.4, "Configuring the Policy and Credential Store to Use OID"](#).

The policy store can be configured to use Oracle Internet Directory 11gR1 and 10.1.4.3, and OVD 11gR1 with the Local Store Adapter (LSA).

The identity store can be configured to use the following LDAP servers:

- Oracle Internet Directory (OID) 11gR1 and 10.1.4.3
- Oracle Virtual Directory (OVD) 11gR1 and 10.1.4
- Sun iPlanet version 4.1.3
- Active Directory shipped as part of Windows 2000
- Open LDAP version 2.0.7
- Novell NDS version 8.5.1

For more information on reconfiguring the identity and policy stores, see [Section 14.3, "Configuring the Identity Store"](#) and [Section 14.4, "Configuring the Policy and Credential Store to Use OID"](#).

---

---

**Note:** The Oracle Content Server and Oracle WebCenter Discussions back-ends can only be configured to use an external LDAP-based identity store. Consequently, the Documents service, which relies on the Oracle Content Server back-end, requires that you reassociate the identity store with one of the external LDAP servers listed above. It is also recommended that WebCenter Spaces and the Oracle Content Server share the same LDAP server.

---

---

#### 14.2.3.1 File-based Credential Store

The out-of-the-box credential store is wallet-based (that is, file-based) and is contained in the file `cwallet.sso`. The location of this file is specified in the Oracle Platform Security configuration file `jps-config.xml`. When you reassociate the policy store to an LDAP directory, the application credentials are automatically migrated to the same LDAP directory as the policy store.

## 14.2.4 Default Policy Store Permissions and Grants

The ADF Security permissions model supports both permission-based and role-based authorization. These two types of authorization are discussed in the following sections:

- [Permission-based Authorization](#)
- [Role-mapping Based Authorization](#)

### 14.2.4.1 Permission-based Authorization

Use permission-based authorization for services, such as the Lists service, where access control is implemented within the WebCenter application using Oracle Platform Security Services (OPSS). WebCenter Spaces provides extensive user and role management tools with which you can create application roles, and define what permissions should be granted to those roles. For information on managing users and roles in WebCenter Spaces, see [Managing Application Roles and Permissions](#).

### 14.2.4.2 Role-mapping Based Authorization

Services that need to access "remote" (back-end) resources require role-mapping based authorization. For example, for the Discussions service, role mapping is required when the users of a WebCenter application (mapping to one or more group space roles) need to be mapped to another set of roles on the Oracle WebCenter Discussions Server (or Oracle Content Server).

The following points should be considered when provisioning role-mapping based authorization in WebCenter Spaces:

- Default application and group space roles for WebCenter Spaces are mapped to the corresponding service roles (see [Table 14-1, "WebCenter Role Permissions"](#) for the default mappings).
- When a new user is granted an application or group space role, a similar grant (privilege) is granted in the back-end server. For example, when user Pat is granted `Discussions-Manage` permissions in WebCenter Spaces, Pat is granted corresponding permissions in the back-end discussion server. See also, [Section 19.1.4, "Understanding Discussions Server Role and Permission Mapping"](#).

### 14.2.4.3 Default Policy Store Permissions for WebCenter Spaces

[Table 14-1](#) shows the pre-seeded roles in the WebCenter policy store (WebCenter Seeded Roles). The Community of Interest Role Template and Group Space Project Role Template are policy entries that are kept in the corresponding group space templates. When a new group space is created, the roles and corresponding permissions are added to the policy store at runtime.

**Table 14-1 WebCenter Role Permissions**

| Permission grants to roles in WebCenter | WebCenter - admin | Spaces-User | Public-User | Community of Interest | Community of Interest | Community of Interest | Group Space Project | Group Space Project | Group Space Project |
|---|-------------------|-------------|-------------|-----------------------|-----------------------|-----------------------|---------------------|---------------------|---------------------|
| Role Mapping                            |                   |             |             | moderator             | participant           | viewer                | moderator           | participant         | viewer              |
| WebCenterPermission (Application)       |                   |             |             |                       |                       |                       |                     |                     |                     |
| manage                                  | ✓                 |             |             |                       |                       |                       |                     |                     |                     |
| configure                               | +                 |             |             |                       |                       |                       |                     |                     |                     |
| view                                    | +                 | ✓           | ✓           |                       |                       |                       |                     |                     |                     |

**Table 14–1 (Cont.) WebCenter Role Permissions**

| Permission grants to roles in WebCenter | WebCenter - admin | Spaces-User | Public-User | Community of Interest moderator | Community of Interest participant | Community of Interest viewer | Group Space Project moderator | Group Space Project participant | Group Space Project viewer |
|---|-------------------|-------------|-------------|---------------------------------|-----------------------------------|------------------------------|-------------------------------|---------------------------------|----------------------------|
| <b>SpacePermission (Group Spaces)</b>   |                   |             |             |                                 |                                   |                              |                               |                                 |                            |
| manage                                  | ✓                 |             |             | ✓                               |                                   |                              | ✓                             |                                 |                            |
| configure                               | +                 |             |             | +                               |                                   |                              | +                             |                                 |                            |
| view                                    | +                 |             |             | +                               | ✓                                 | ✓                            | +                             | ✓                               | ✓                          |
| create                                  | +                 | ✓           |             |                                 |                                   |                              |                               |                                 |                            |
| <b>PagePermission (Page)</b>            |                   |             |             |                                 |                                   |                              |                               |                                 |                            |
| manage                                  | ✓                 |             |             | ✓                               |                                   |                              | ✓                             |                                 |                            |
| create                                  | +                 | ✓           |             | +                               |                                   |                              | +                             |                                 |                            |
| delete                                  | +                 |             |             | +                               |                                   |                              | +                             |                                 |                            |
| edit                                    | +                 |             |             | +                               |                                   |                              | +                             |                                 |                            |
| personalize                             | +                 |             |             | +                               |                                   |                              | +                             |                                 | ✓                          |
| view                                    | +                 |             |             | +                               | ✓                                 | ✓                            | +                             | ✓                               | ✓                          |
| <b>ListPermission* (Lists)</b>          |                   |             |             |                                 |                                   |                              |                               |                                 |                            |
| manage                                  |                   |             |             | ✓                               |                                   |                              | ✓                             |                                 |                            |
| create                                  |                   |             |             | +                               | ✓                                 |                              | +                             | ✓                               |                            |
| delete                                  |                   |             |             | +                               | ✓                                 |                              | +                             | ✓                               |                            |
| edit                                    |                   |             |             | +                               | ✓                                 |                              | +                             | ✓                               |                            |
| update                                  |                   |             |             | +                               | ✓                                 |                              | +                             | ✓                               | ✓                          |
| view                                    |                   |             |             | +                               | ✓                                 | ✓                            | +                             | ✓                               | ✓                          |
| <b>EventPermission (Events)</b>         |                   |             |             |                                 |                                   |                              |                               |                                 |                            |
| manage                                  |                   |             |             | ✓                               |                                   |                              | ✓                             |                                 |                            |
| create                                  |                   |             |             | +                               | ✓                                 |                              | +                             | ✓                               |                            |
| delete                                  |                   |             |             | +                               | ✓                                 |                              | +                             | ✓                               |                            |
| edit                                    |                   |             |             | +                               | ✓                                 |                              | +                             | ✓                               |                            |
| view                                    |                   |             |             | +                               | ✓                                 | ✓                            | +                             | ✓                               | ✓                          |
| <b>NotePermission (Notes)</b>           |                   |             |             |                                 |                                   |                              |                               |                                 |                            |
| manage                                  |                   |             |             | ✓                               |                                   |                              | ✓                             |                                 |                            |
| create                                  |                   |             |             | +                               | ✓                                 |                              | +                             | ✓                               |                            |
| delete                                  |                   |             |             | +                               | ✓                                 |                              | +                             | ✓                               |                            |
| update                                  |                   |             |             | +                               | ✓                                 |                              | +                             | ✓                               |                            |
| view                                    |                   |             |             | +                               | ✓                                 | ✓                            | +                             | ✓                               | ✓                          |
| <b>Discussions</b>                      |                   |             |             |                                 |                                   |                              |                               |                                 |                            |

**Table 14–1 (Cont.) WebCenter Role Permissions**

| Permission grants to roles in WebCenter                                    | WebCenter - admin | Spaces-User | Public-User | Community of Interest moderator | Community of Interest participant | Community of Interest viewer | Group Space Project moderator | Group Space Project participant | Group Space Project viewer |
|--|-------------------|-------------|-------------|---------------------------------|-----------------------------------|------------------------------|-------------------------------|---------------------------------|----------------------------|
| manage (Forum Moderator Role)  | ✓                 |             |             | ✓                               |                                   |                              | ✓                             |                                 |                            |
| edit (Forum Writer Role)   |                   |             |             | +                               | ✓                                 |                              | +                             | ✓                               |                            |
| view (Forum Reader Role)   |                   |             |             | +                               |                                   | ✓                            | +                             |                                 | ✓                          |
| Document Library roles (Role id/Enum name/short description)** (Documents) |                   |             |             |                                 |                                   |                              |                               |                                 |                            |
| 1/SUPER_ADMINISTRATOR (manage)   |                   |             |             |                                 |                                   |                              |                               |                                 |                            |
| 2/DELETE (delete)  |                   |             |             | ✓                               |                                   |                              | ✓                             |                                 |                            |
| 3/WRITE (create)   |                   |             |             | ✓                               | ✓                                 |                              | ✓                             | ✓                               |                            |
| 4/READ (view)  |                   |             |             | ✓                               | ✓                                 | ✓                            | ✓                             | ✓                               | ✓                          |
| Announcements  |                   |             |             |                                 |                                   |                              |                               |                                 |                            |
| manage   |                   |             |             | ✓                               |                                   |                              | ✓                             |                                 |                            |
| edit   |                   |             |             | +                               | ✓                                 |                              | +                             | ✓                               |                            |
| view   |                   |             |             | +                               |                                   | ✓                            | +                             |                                 | ✓                          |
| Links  |                   |             |             |                                 |                                   |                              |                               |                                 |                            |
| manage   | ✓                 |             |             | ✓                               |                                   |                              | ✓                             |                                 |                            |
| delete   |                   |             |             | +                               | ✓                                 |                              | +                             | ✓                               |                            |
| create   |                   |             |             | +                               |                                   | ✓                            | +                             |                                 | ✓                          |
| ProfilePermission  |                   |             |             |                                 |                                   |                              |                               |                                 |                            |
| manage   | ✓                 |             |             |                                 |                                   |                              |                               |                                 |                            |
| edit   | +                 | ✓           |             |                                 |                                   |                              |                               |                                 |                            |

\* For the Lists service, "Edit" means the ability to edit a definition as well as content, and "update" means the ability to edit content. "Manage", for lists and elsewhere in this table, means the ability to make configuration and security changes.

\*\* The Documents service uses integer identifiers for roles. The role mapping information in the policy store therefore refers to the corresponding service role's integer identifier. Each service role has an associated short and long description. The WebCenter security provisioning screens show the corresponding description instead of IDs.

| Legend | Description   |
|--------|---|
| ✓      | Shows an explicitly granted permission, action, or role mapping.  |
| +      | Shows an implied permission as a result of an explicitly granted permission. The permission implementation itself does the implication. |

#### 14.2.4.4 Default Code-based Grants

Some WebCenter application and framework code calls APIs from the security platform that are secured with Permission checks. The WebCenter code needs to be granted the appropriate permissions to invoke the OPSS APIs, and itself should authorize access to the various operations exposed in the User Interface. For example, the permission to access policy store and grant or revoke permissions (`PolicyStoreAccessPermission`), CRUD on application roles, is granted to the "webcenter" application out of the box. The WebCenter code must then pre-authorize access to the various operations, using the above WebCenter-specific permissions, and then invoke the OPSS APIs as privileged actions.

### 14.2.5 Post-deployment Security Configuration Tasks

After deploying your WebCenter application, consider the following configuration tasks for your site:

- **SSL**

Secure Sockets Layer (SSL) provides additional security for connections between WebCenter applications or components by providing an additional authentication layer, and by encrypting the data exchanged. For connections between applications or components where the data exchanges is sensitive, consider securing the connection with SSL. For a list of the connections that can and should be protected with SSL in a production environment, see [Section 14.6, "Configuring WebCenter Applications and Components to Use SSL"](#).

---

---

**Note:** Using SSL is computationally intensive and adds overhead to a connection. SSL should therefore not be used where it is not required, and is best reserved for production environments.

---

---

- **SSO**

Single Sign-On (SSO) allows users to log in once across WebCenter applications and components rather than having to log in for each sub-application (for example, for accessing a wiki page in WebCenter Spaces). Users do not have to maintain a separate user ID and password for each application or component that they access. However, you can still configure a variety of authentication methods, so that more sensitive applications can be protected using more stringent methods. WebCenter supports four single sign-on solutions: Oracle Access Manager (OAM), Oracle Single Sign-on (OSSO), a SAML-based single sign-on solution for Oracle WebCenter applications only, and an SSO solution for Microsoft clients, using Windows authentication based on the Simple and Protected Negotiate (SPNEGO) mechanism and the Kerberos protocol. For a discussion of these solutions and an overview of single sign-on, see [Section 14.7, "Configuring a WebCenter Application to Use Single Sign-On"](#).

- **Reassociate the identity store to use an external LDAP**

By default, WebCenter applications use an embedded LDAP for its identity store. Although secure, the out-of-the-box embedded LDAP may not scale appropriately for large enterprise production environments. For instructions on how to configure the identity store to use an external LDAP such as Oracle Internet Directory (OID), see [Section 14.3, "Configuring the Identity Store"](#).

---

---

**Note:** Oracle Content Server and Oracle WebCenter Discussions Server must use an external LDAP identity store rather than the default embedded LDAP identity store. Consequently, if you plan on using the Documents or Discussions services in your WebCenter application, you must reconfigure the identity store to use an external LDAP. For more information on reconfiguring the identity store, see [Section 14.3, "Configuring the Identity Store"](#).

---

---

- **Reassociate the policy store to use an external LDAP**

By default, WebCenter uses a file-based `system-jazn-data.xml` policy store to store policy grants. You should consider using an LDAP-based policy store. For information on how to configure the policy store to use LDAP, see [Section 14.4, "Configuring the Policy and Credential Store to Use OID"](#).

- **WS-Security**

Although the use of WS-Security adds complexity to the configuration and management of a WebCenter application and the set of producers it consumes, it helps ensure the security of the information being published by the WebCenter application. Adding WS-Security provides authentication for the consumer, and message-level security.

For information on how to configure WS-Security for WebCenter applications and components, see [Section 14.8, "Configuring WS-Security"](#).

## 14.3 Configuring the Identity Store

This section describes how to reassociate the identity store with an external LDAP rather than the default embedded identity store. It also provides additional configuration information for configuring services such as the discussions server, and contains the following subsections:

- [Section 14.3.1, "Reassociating the Identity Store with an External LDAP"](#)
- [Section 14.3.2, "Tuning the Identity Store for Performance"](#)
- [Section 14.3.3, "Adding Users to the Identity Store"](#)
- [Section 14.3.4, "Moving the Administrator Account to an External LDAP Server"](#)
- [Section 14.3.5, "Granting the WebCenter Administrator Role to a WebCenter Spaces User"](#)
- [Section 14.3.6, "Configuring the Discussions Server to Share the Identity Store LDAP Server"](#)
- [Section 14.3.7, "Configuring the Discussions Server to Share the Identity Store Embedded LDAP Server"](#)
- [Section 14.3.8, "Configuring the Oracle Content Server to Share the Identity Store LDAP Server"](#)

Note that for custom WebCenter applications, the steps for [Granting the WebCenter Administrator Role to a WebCenter Spaces User](#) and [Configuring the Discussions Server to Share the Identity Store LDAP Server](#) are not required. For more information about the identity store, see the *Oracle Fusion Middleware Security Guide*.

---

---

**Caution:** Before reassociating the identity store, be sure to back up the relevant configuration files:

- `config.xml`
- `jps-config.xml`
- `system-jazn-data.xml`

As a precaution, you should also back up the `boot.properties` file for the domain Administration Server for the domain.

---

---

### 14.3.1 Reassociating the Identity Store with an External LDAP

This section describes how to configure the identity store to use an external LDAP server, such as Oracle Internet Directory, rather than the default embedded LDAP.

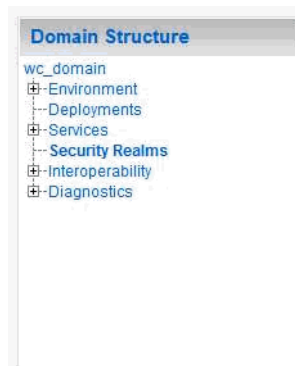
To reassociate the identity store:

1. Log in to the WLS Administration Console.

For information on logging into the WLS Administration Console, see [Section 1.12.2, "Oracle WebLogic Server Administration Console"](#).

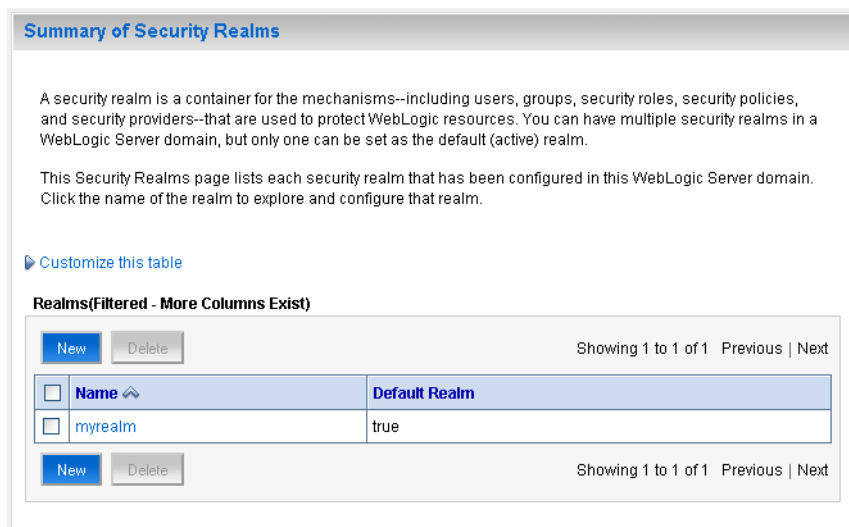
2. In the Domain Structure pane (see [Figure 14-12](#)), click **Security Realms**.

**Figure 14-4 Domain Structure Pane**



The Summary of Security Realms pane displays (see [Figure 14-13](#)).

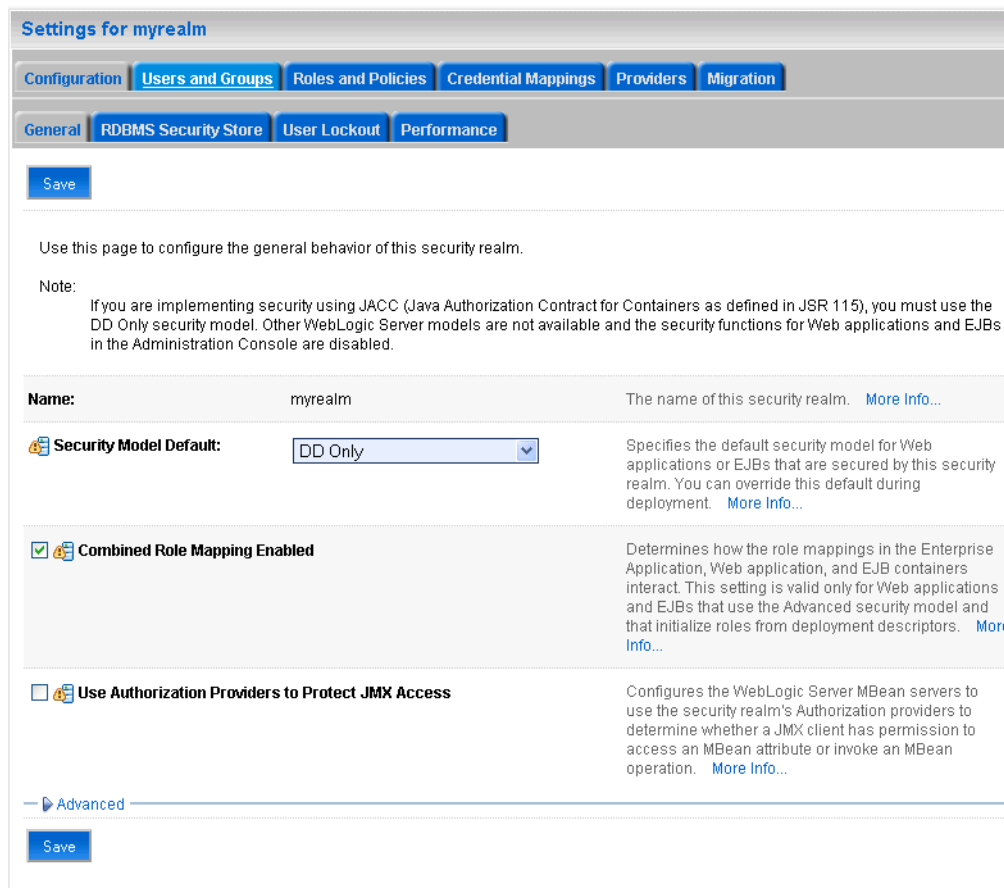
**Figure 14–5 Summary of Security Realms pane**



3. In the Name column, click the realm for which you want to reassociate the identity store.

The Realm Settings pane displays (see [Figure 14–6](#)).

**Figure 14–6 Realm Settings Pane**





4. Open the **Providers** tab.

The Providers Settings pane displays (see [Figure 14-7](#)).

**Figure 14-7 Settings Pane - Providers**

Settings for myrealm

Configuration Users and Groups Roles and Policies Credential Mappings **Providers** Migration

**Authentication** Authorization Adjudication Role Mapping Auditing Credential Mapping Certification Path Keystores

An Authentication provider allows WebLogic Server to establish trust by validating a user. You must have one Authentication provider in a security realm, and you can configure multiple Authentication providers in a security realm. Different types of Authentication providers are designed to access different data stores, such as LDAP servers or DBMS. You can also configure a Realm Adapter Authentication provider that allows you to work with users and groups from previous releases of WebLogic Server.

[Customize this table](#)

**Authentication Providers**

New Delete Reorder Showing 1 to 2 of 2 Previous | Next

| <input type="checkbox"/> | Name                    | Description                          | Version |
|--------------------------|-------------------------|--------------------------------------|---------|
| <input type="checkbox"/> | DefaultAuthenticator    | WebLogic Authentication Provider     | 1.0     |
| <input type="checkbox"/> | DefaultIdentityAsserter | WebLogic Identity Assertion provider | 1.0     |

New Delete Reorder Showing 1 to 2 of 2 Previous | Next

5. Click **New** to add a new provider.

The Create a New Authentication Provider pane displays (see [Figure 14-8](#)).

**Figure 14-8 Create a New Authentication Provider Pane**

Create a New Authentication Provider

OK Cancel

**Create a new Authentication Provider**

The following properties will be used to identify your new Authentication Provider.  
\* Indicates required fields

The name of the authentication provider.

\* Name:

This is the type of authentication provider you wish to create.

Type:

OK Cancel

6. Enter a name for the provider (for example `OIDAuthenticator` for a provider that will authenticate the user for the Oracle Internet Directory).
7. Select the authenticator appropriate for your LDAP directory from the list of authenticators.

Be sure to select the authenticator associated with the LDAP you are configuring rather than choosing the generic `DefaultAuthenticator`. For example, for OID

select `OracleInternetDirectoryAuthenticator`, or for iPlanet select `iPlanetAuthenticator`. Move the authenticator to the top of the authenticator list and set its Control Flag (and any other authenticator Control Flags in the list), to `SUFFICIENT`.

See [Section 14.3.4, "Moving the Administrator Account to an External LDAP Server"](#) for information about how to configure the default administrator account.

---

**Note:** If more than one authenticator is configured, WebCenter Spaces will work only with the users in the identity store mapped by the first authenticator.

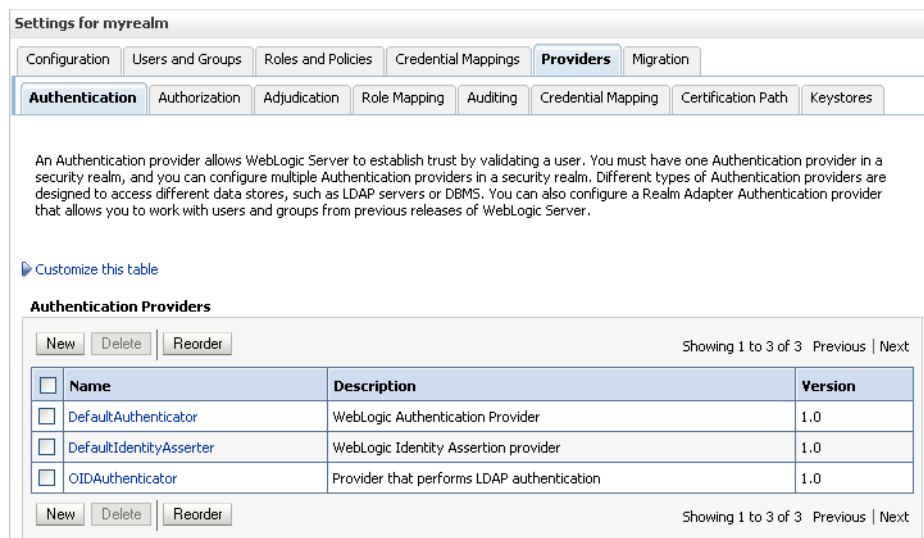
The identity store access APIs use the first `REQUIRED` authenticator in the list. If there are no `REQUIRED` authenticators, it uses the first `SUFFICIENT` one. Therefore, for stacked authenticators, be sure to list the authenticator mapping the primary identity store to be used with the identity store access APIs first, and set all other authenticator control flags to `SUFFICIENT`.

---

8. Click **OK** to save your settings.

The Settings pane displays with the new authentication provider (see [Figure 14–9](#)).

**Figure 14–9 Settings Pane - Authentication Providers**



9. In the list of Authentication Providers, click the newly created provider.

The Settings Pane for the new authentication provider displays (see [Figure 14–10](#)).

**Figure 14–10 Settings Pane for Authenticator**

Settings for OIDAAuthenticator

Configuration Performance

Common Provider Specific

Save

Use this page to define the general configuration of this Oracle Internet Directory Authentication provider.

|               |  |   |
|---------------|--|---|
| Name:         | OIDAuthenticator                           | The name of this Oracle Internet Directory Authentication provider. <a href="#">More Info...</a>                                |
| Description:  | Provider that performs LDAP authentication | A short description of this Oracle Internet Directory Authentication provider. <a href="#">More Info...</a>                     |
| Version:      | 1.0  | The version number of this Oracle Internet Directory Authentication provider. <a href="#">More Info...</a>                      |
| Control Flag: | SUFFICIENT                                 | Specifies how this Oracle Internet Directory Authentication provider fits into the login sequence. <a href="#">More Info...</a> |

Save

**10.** Set the Control Flag to SUFFICIENT.

Setting the Control Flag to SUFFICIENT indicates that if a user can be authenticated successfully by this authenticator, then the authentication provider should accept that authentication and should not invoke any additional authenticators.

---

**Note:** If the authentication fails, it will fall through to the next authenticator in the chain. Therefore, be sure all subsequent authenticators also have their control flag set to SUFFICIENT.

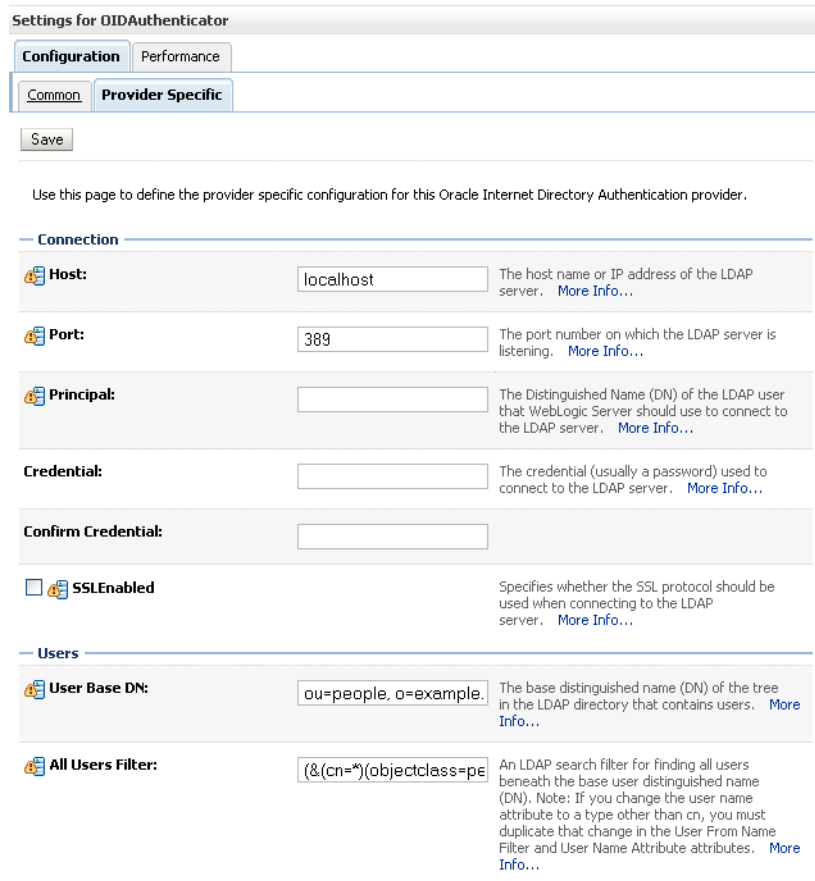
---

**11.** Click **Save** to save this setting.

**12.** Open the Provider Specific tab to enter the details for the LDAP server.

The Provider Specific pane displays (see [Figure 14–11](#)).

**Figure 14–11 Provider Specific Pane**



This screenshot shows the Provider Specific authenticator settings pane.

\*\*\*\*\*

13. Enter the details specific to *your* LDAP server.

| Parameter                            | Value   | Description   |
|--------------------------------------|---------|---|
| Host:                                |         | The LDAP server's server ID (for example, <code>&lt;ldap_host&gt;example.com</code> )                   |
| Port:                                |         | The LDAP server's port number (for example, 3060)   |
| Principal:                           |         | The LDAP user DN used to connect to the LDAP server (for example, <code>cn=orcladmin</code> )           |
| Credential:                          |         | The password used to connect to the LDAP server   |
| User Base DN:                        |         | Specify the DN under which your Users start (for example, <code>cn=users,dc=example,dc=com</code> )     |
| Group Base DN:                       |         | Specify the DN that points to your Groups node (for example, <code>cn=groups,dc=example,dc=com</code> ) |
| Use Retrieved User Name as Principal | Checked | Must be turned on   |

| Parameter              | Value                              | Description  |
|------------------------|------------------------------------|--|
| All Users Filter:      | ( &(uid=*) (objectclass=person) )  | Search to find all users under the <b>User Base DN</b> |
| User From Name Filter: | ( &(uid=%u) (objectclass=person) ) |  |
| User Name Attribute:   | uid                                |  |

If you modify a username attribute to something other than the default set for the LDAP server in the authenticator, you must also edit the `jps-config.xml` file to correspond to these values. Specifically, the **username.attr** and **user.login.attr** properties (highlighted below) must be added for user lookups to function correctly:

```
<!-- JPS WLS LDAP Identity Store Service Instance -->
<serviceInstance name="idstore.ldap" provider="idstore.ldap.provider">
<property name="idstore.config.provider"
value="oracle.security.jps.wls.internal.idstore.WlsLdapIdStoreConfigProvider"/>
<property name="username.attr" value="uid"/>
<property name="user.login.attr" value="uid"/>
</serviceInstance>
```

14. Click **Save**.

15. Return to the Providers tab and reorder the providers so that the new authentication provider is on top, followed by any other authenticators with the `DefaultAuthenticator` placed at the end of the list.

All should have their Control Flags set to `SUFFICIENT` so that subsequent authenticators can authenticate identities that fall through from the new provider all the way through to the `DefaultAuthenticator` (which is used only for the default file-based embedded LDAP). For example, logins such as the default administrator account are not typically created in the LDAP directory, but still need to be authenticated to start up the server. Unless identities are allowed to fall through to the `DefaultAuthenticator`, the default administrator account will not be authenticated. For more information about the `DefaultAuthenticator` and the default administrator account, see [Section 14.3.4, "Moving the Administrator Account to an External LDAP Server"](#).

16. Restart the Administration Server and the managed server for the changes to take effect.

### 14.3.2 Tuning the Identity Store for Performance

For a production environment, we recommended that you add the following configuration entry to the `jps-config.xml` file for best performance:

```
<serviceInstance provider="idstore.ldap.provider" name="idstore.ldap">
<property
value="oracle.security.jps.wls.internal.idstore.WlsLdapIdStoreConfigProvider"
name="idstore.config.provider"/>
<property name="CONNECTION_POOL_CLASS"
value="oracle.security.idm.providers.stdlldap.JNDIPool"/>
</serviceInstance>
```

### 14.3.3 Adding Users to the Identity Store

You can add users to the embedded LDAP or an external LDAP using the WLS Administration Console. For Oracle Internet Directory, although users are typically managed using ODSM (described in the section on "Managing Directory Entries" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*), you can also use the WLS Administration Console as described below.

---

---

**Note:** If you are planning to reassociate your identity store with an external LDAP, carry out that step (as described in [Section 14.3.1, "Reassociating the Identity Store with an External LDAP"](#)) prior to adding users to avoid having to migrate the users from the embedded LDAP to the newly configured external LDAP.

---

---

For WebCenter Spaces, users who self-register are added directly to the identity store. For more information about self-registration, see [Section 19.4, "Allowing Self-Registration"](#).

You can also add users directly into the embedded LDAP identity store using an LDIF file and LDAP commands. Using an LDIF file lets you add additional attributes not available through the WLS Administration Console.

---

---

**Note:** Adding users to the identity store is typically a system administrator task and may not be a task for which application-level administrators have the required permissions.

---

---

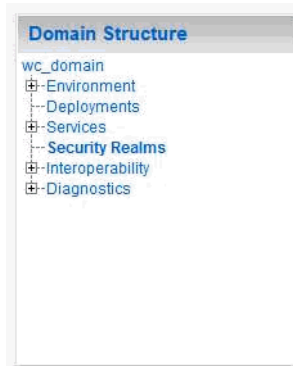
This section includes the following subsections:

- [Adding Users Using the WLS Administration Console](#)
- [Adding Users to the Embedded LDAP Using an LDIF File](#)

#### 14.3.3.1 Adding Users Using the WLS Administration Console

To add users to the embedded LDAP or to an external LDAP from the WLS Administration Console:

1. Log in to the WLS Administration Console.  
For information on logging into the WLS Administration Console, see [Section 1.12.2, "Oracle WebLogic Server Administration Console"](#).
2. In the Domain Structure pane (see [Figure 14-12](#)), click **Security Realms**.

**Figure 14–12 Domain Structure Pane**

The Summary of Security Realms pane displays (see [Figure 14–13](#)).

**Figure 14–13 Summary of Security Realms pane**

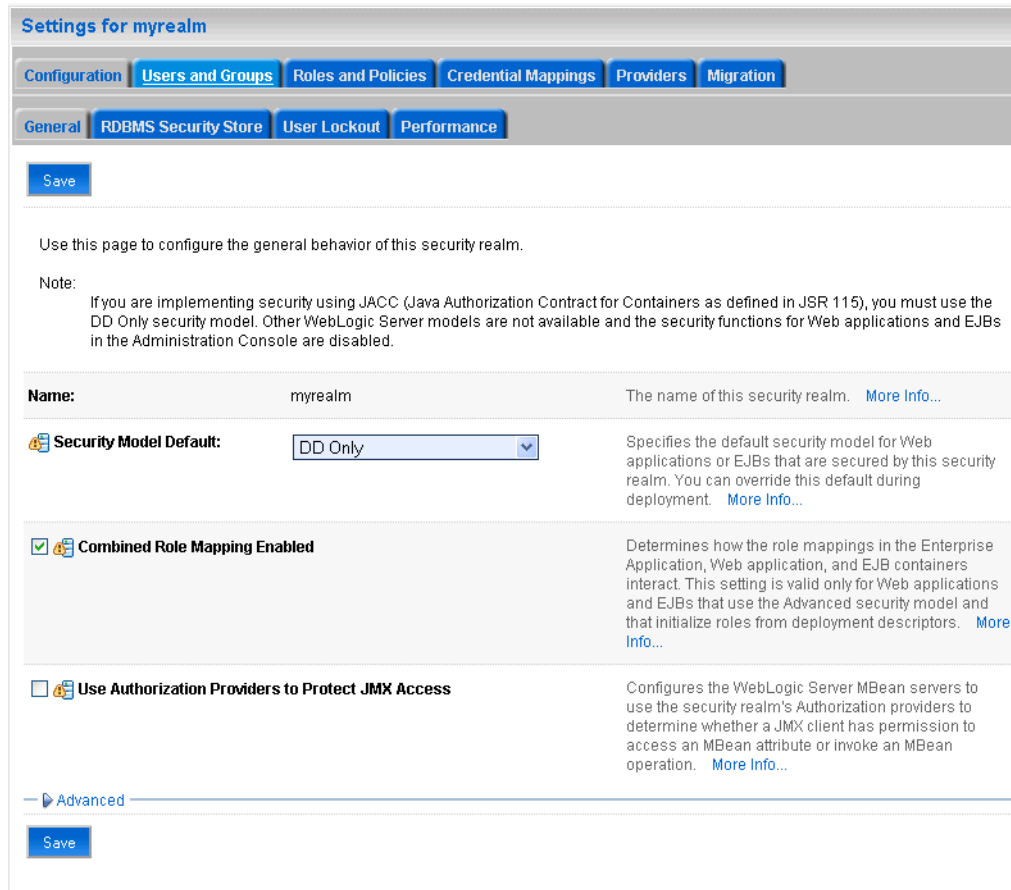
The screenshot shows the "Summary of Security Realms" pane. It contains an introductory paragraph explaining that a security realm is a container for mechanisms like users, groups, security roles, security policies, and security providers. It also states that multiple security realms can exist in a WebLogic Server domain, but only one can be the default (active) realm. Below the text is a link to "Customize this table".

The main content is a table titled "Realms(Filtered - More Columns Exist)". The table has two columns: "Name" and "Default Realm". There is one row with the name "myrealm" and the value "true". Above and below the table are "New" and "Delete" buttons, and "Showing 1 to 1 of 1 Previous | Next" text.

| Name    | Default Realm |
|---------|---------------|
| myrealm | true          |

3. In the Name column, click the realm to which you want to add users.  
The Realm Settings pane displays (see [Figure 14–14](#)).

**Figure 14–14 Realm Settings Pane**



4. Click the **Users and Groups** tab to display the list of current users.
5. Click **New** to add a new user.



Figure 14–15 Create a New User Page

**Create a New User**

OK Cancel

**User Properties**

The following properties will be used to identify your new User.  
\* Indicates required fields

What would you like to name your new User?

\* **Name:**

How would you like to describe the new User?

**Description:**

Please choose a provider for the user.

**Provider:**

The password is associated with the login name for the new User.

**Password:**

**Confirm Password:**

OK Cancel

This screenshot shows the Create a New User page.

\*\*\*\*\*

6. On the Create a New User page, enter the new user login name in the **Name** field.

User names are case sensitive and must be unique. Do not use commas, tabs or any other characters in the following comma-separated list:

<>, #, |, &, ?, (, { }

7. In the **Description** field, enter a description for the user (for example, the user's full name).
8. From the **Provider** drop-down menu, select the Authentication provider for the user.

If multiple WebLogic Authentication providers are configured in the security realm, they will appear in the list. For the embedded LDAP, choose `DefaultAuthenticator`; for Oracle Internet Directory, choose `OracleInternetDirectoryAuthenticator`. For other external LDAPs, choose the authenticator associated with that LDAP.

9. In the **Password** field, enter a password for the user.

The minimum password length for a user defined in the WebLogic Authentication provider is 8 characters (note that other LDAP providers may have different requirements for the password length). Do not use user name/password combinations such as `weblogic/weblogic` in a production environment.

10. Re-enter the password in the **Confirm Password** field.
11. Click **OK** to save your changes and add the user.

The user should now appear in the list of users.

### 14.3.3.2 Adding Users to the Embedded LDAP Using an LDIF File

To add users to the embedded LDAP using an LDIF file you need to carry out the following tasks:

- [Enable External LDAP Access](#)
- [Create an LDIF File](#)
- [Add the Users](#)

The WLS Administration Console does not provide support for adding any additional attributes. However, the embedded LDAP server is in fact, a proper LDAP server, and so you can use LDAP commands to add or modify users. You can also search the directory, which can be useful when exporting and importing user accounts.

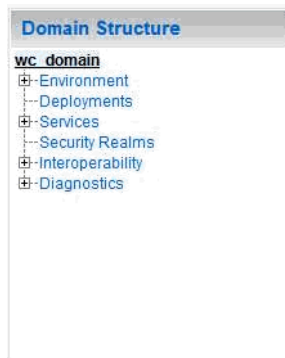
#### Enable External LDAP Access

When WLS is installed, the LDAP access credential is set as a randomized value and encrypted in the `config.xml` file. To enable external LDAP access, you need to reset the access credential for the embedded LDAP.

To reset the access credential for the embedded LDAP:

1. Log in to the WLS Administration Console.  
For information on logging into the WLS Administration Console, see [Section 1.12.2, "Oracle WebLogic Server Administration Console"](#).
2. In the Domain Structure pane (see [Figure 14–16](#)), click on `wc_domain`.

**Figure 14–16 Domain Structure Pane (`wc_domain`)**



3. In the Settings pane for `wc_domain`, click the Security tab, and then click the Embedded LDAP tab.

The Settings Pane for `wc_domain` displays the embedded LDAP settings (see [Figure 14–17](#)).

**Figure 14–17 Settings Pane with Embedded LDAP Settings**

4. Enter a new password in the **Credential** field, and re-enter it in the **Confirm Credential** field.
5. Click **Save** to save your settings.
6. Restart the WebLogic server.

After this, you are ready to access the LDAP server with the following values:

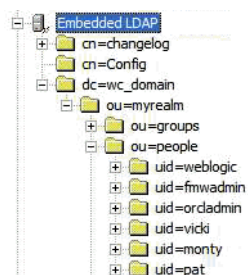
- the DN value for admin access is "cn=Admin"
- the password is the value you entered in the Credential field
- the port is the same as the admin port, which by default is 7001

### Create an LDIF File

You can create an LDIF file with any text editor, and can include any attributes appropriate for the embedded LDAP directory. The `objectclasses` that are supported by default in the embedded LDAP server for WLS are the following:

- `person`
- `inetOrgPerson`
- `organizationalPerson`
- `wlsUser`

In order to interact successfully with the embedded LDAP server, you should understand the default layout of the directory information tree (DIT). The default layout in the embedded LDAP directory is shown in [Figure 14–18](#).

**Figure 14–18 Embedded LDAP Directory Information Tree**

This graphic shows an expanded embedded LDAP Directory Information Tree.

\*\*\*\*\*

---



---

**Note:** The naming attribute for the user entry in the embedded LDAP directory tree is "uid". This is different from the default configuration for Oracle Internet Directory (OID), where the naming attribute is "cn". Also, the location of the users in this tree is "ou=people,ou=myrealm,dc=wc\_domain".

---



---

The following example shows an LDIF file with the attributes that are displayed in the WebCenter Spaces Profile Details screen:

```
dn: uid=john.doe,ou=people,ou=myrealm,dc=wc_domain
description: John Doe
cn: john.doe
uid: john.doe
sn: Doe
objectclass: wlsUser
objectclass: organizationalperson
objectclass: inetOrgPerson
objectclass: person
objectclass: top
userpassword: welcome1
displayName: John Doe
employeeNumber: 12345
employeeType: Regular
givenName: John
homePhone: 650-555-1212
mail: john.doe@example.com
title: Manager
manager: uid=mary.jones,ou=people,ou=myrealm,dc=wc_domain
preferredLanguage: en
departmentNumber: tools
facsimiletelephonenumber: 650-555-1200
mobile: 650-500-1200
pager: 650-400-1200
telephoneNumber: 650-506-1212
postaladdress: 200 Oracle Parkway
l: Redwood Shores
homepostaladdress: 123 Main St., Anytown 12345
```

To create a file with multiple user entries, just replicate the above lines as many times as required, with a blank line between entries.

---



---

**Note:** Note that the WebCenter Spaces Profile Details screen also lists some attributes that are only available in an Oracle Internet Directory. These cannot be entered when using the embedded LDAP identity store. These include the following attributes, from the `orclUserV2` objectclass:

- `orclTimeZone`
  - `orclDateOfBirth`
  - `maidenName`
- 
-

## Add the Users

The example below uses the `ldappadd` command, a part of the LDAP command line utilities provided with the Oracle Internet Directory server. For more information about using the `ldappadd` command, see "Oracle Internet Directory Data Management Tools" in the *Oracle Fusion Middleware User Reference for Oracle Identity Management*.

```
ldappadd -h weblogichost.example.com -p 7001 -D cn=Admin -w password -v -f
newuser.ldif
```

```
add description:
    John Doe
add cn:
    john.doe
add uid:
    john.doe
add sn:
    Doe
add objectclass:
    wlsUser
    organizationalperson
    inetOrgPerson
    person
    top
add userpassword:
    password
add displayname:
    John Doe
add employeenumbr:
    12345
add employeetype:
    Regular
add givenname:
    John
add homephone:
    650-555-1212
add mail:
    john.doe@example.com
add title:
    Manager
add manager:
    uid=mary.jones,ou=people,ou=myrealm,dc=wc_domain
add preferredlanguage:
    en
add departmentnumber:
    tools
add facsimiletelephonenumber:
    650-555-1200
add mobile:
    650-500-1200
add pager:
    650-400-1200
add telephonenumber:
    650-506-1212
add postaladdress:
    200 Oracle Parkway
add l:
    Redwood Shores
add homepostaladdress:
    123 Main St., Anytown 12345
```

```
adding new entry uid=john.doe,ou=people,ou=myrealm,dc=wc_domain
modify complete
```

### 14.3.4 Moving the Administrator Account to an External LDAP Server

When configuring the domain to use an external LDAP server, you can also optionally move the administrator account (`weblogic` by default) to the LDAP server.

If the administrator account, or any other appropriate user in LDAP, is in an LDAP group called "Administrators", then this account should be sufficient to manage the server, and the `DefaultAuthenticator` provider can be removed from the list of authentication providers. In this case, all users and including the administrator account are looked up from the external LDAP.

If you cannot create the `weblogic` (default) user in the external LDAP directory, there are two options. You can:

- Keep the `DefaultAuthenticator` provider and use the `weblogic` account with the local embedded LDAP server in WLS to start and stop servers and do other administrator operations from the WLS Administration Console. If you keep the `DefaultAuthenticator`, make sure that the control flag for the `DefaultAuthentication` provider is set to `SUFFICIENT`.
- Remove the `DefaultAuthenticator` and make sure that any valid user account used for administrator operations, such as starting and stopping servers, is included in an "Administrators" group in Oracle Internet Directory or other named group that contains the list of users that are allowed to manage your domain. If a name other than "Administrators" is used, then you need to update the group name in the definition of the WLS Global Administrator role. By default, this is defined as membership in the enterprise group called "Administrators".

#### Changing the Administrator Group Name

You can change the group name to any other valid enterprise role in your LDAP server that contains users authorized to manage the domain. This lets you delegate the administration of specific domains in your enterprise. You can create various administration groups in the directory and have the corresponding domains be configured to use the appropriate group for defining its administrators.

The following example LDIF file creates an administrative group in Oracle Internet Directory:

```
dn: cn=wc_domain_Admin,cn=groups,dc=example,dc=com
cn: wc_domain_Admin
uniquemember: cn=joe.admin,cn=users,dc=example,dc=com
owner: cn=orcladmin
displayname: WebLogic Administrators Group
description: WebLogic Administrators Group
objectclass: orclgroup
objectclass: groupofuniquenames
```

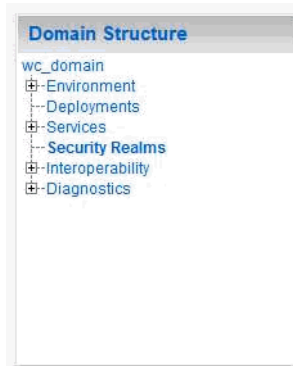
Once this group is created, you need to update the role definition for the WLS Global Admin role in WLS:

To update the role definition for the WLS Global Admin role in WLS

1. Log in to the WLS Administration Console.

For information on logging into the WLS Administration Console, see [Section 1.12.2, "Oracle WebLogic Server Administration Console"](#).

2. In the Domain Structure pane (see [Figure 14–19](#)), click **Security Realms**.

**Figure 14–19 Domain Structure Pane**

The Summary of Security Realms pane displays (see [Figure 14–20](#)).

**Figure 14–20 Summary of Security Realms pane**

The screenshot shows the "Summary of Security Realms" pane. It contains a text block explaining that a security realm is a container for mechanisms like users, groups, security roles, security policies, and security providers. It also states that this page lists each security realm configured in the WebLogic Server domain. Below the text is a link to "Customize this table".

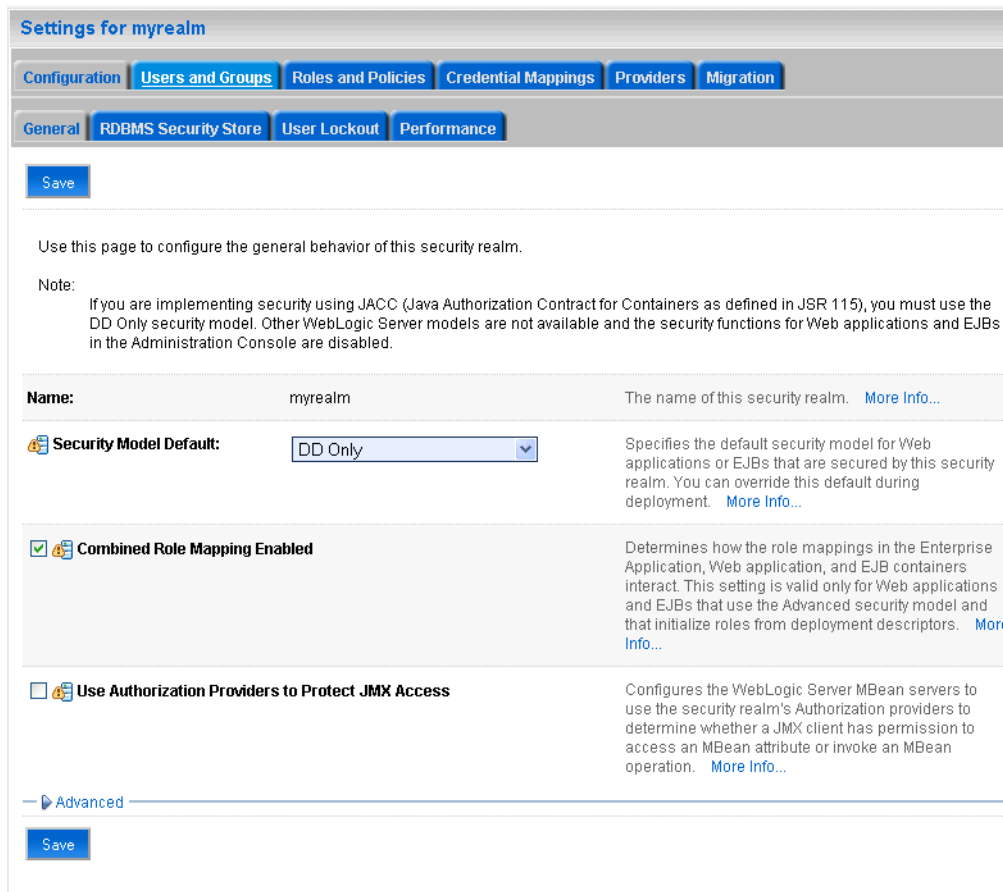
Below the link is a table titled "Realms(Filtered - More Columns Exist)". The table has two columns: "Name" and "Default Realm". There is one row with the name "myrealm" and the value "true".

| Name    | Default Realm |
|---------|---------------|
| myrealm | true          |

3. In the Name column, click the realm for which you want to reassociate the identity store.

The Realm Settings pane displays (see [Figure 14–21](#)).

**Figure 14–21 Realm Settings Pane**



4. Open the Roles and Policies tab, and then the Realm Roles subtab.  
The Realm Roles settings pane displays (see [Figure 14–22](#)).



**Figure 14–22 Realm Roles Settings Pane**

Settings for myrealm

Configuration Users and Groups **Roles and Policies** Credential Mappings Providers Migration

Realm Roles Realm Policies


Use this table to view, add, modify or remove global or scoped security roles for this security realm. Global roles are listed in the Name column under the Global Roles node. Scoped roles are listed in the Name column under the individual resources that they secure.

Notes:

- This table does not list scoped roles for JNDI resources or Work Context resources. To see these scoped roles, view the Security tab for each JNDI node or Work Context object.
- If you imported security roles for EJBs or Web applications from deployment descriptors using the Install Application Assistant, you must activate changes to access the roles.

**Roles**

Edit Role Showing 1 to 7 of 7 Previous | Next

| Name  | Resource Type | Role Policy                          |
|--|---------------|--------------------------------------|
| [-] Deployments  |               |                                      |
| [-] Domain   |               |                                      |
| [-] Global Roles   |               |                                      |
| [-] Roles  |               |                                      |
| Admin  | Global Role   | <a href="#">View Role Conditions</a> |
| AdminChannelUser   | Global Role   | <a href="#">View Role Conditions</a> |
| Anonymous  | Global Role   | <a href="#">View Role Conditions</a> |
| AppTester  | Global Role   | <a href="#">View Role Conditions</a> |
| CrossDomainConnector   | Global Role   | <a href="#">View Role Conditions</a> |
| Deployer   | Global Role   | <a href="#">View Role Conditions</a> |
| Monitor  | Global Role   | <a href="#">View Role Conditions</a> |
| Operator   | Global Role   | <a href="#">View Role Conditions</a> |
| OracleSystemRole   | Global Role   | <a href="#">View Role Conditions</a> |
| [-] JCOM   |               |                                      |
| [-] JDBC   |               |                                      |
| [-] JMS  |               |                                      |
| [-] Servers  |               |                                      |

Edit Role Showing 1 to 7 of 7 Previous | Next

- Expand the Global Roles node, and then the Roles node.
- Click **View Role Conditions** for the `Admin` role.  
The Edit Global Role page displays (see [Figure 14–23](#)).

**Figure 14–23 Edit Global Role Page**

By default, the `Administrators` group in Oracle Internet Directory (or other configured identity store) defines who has the administrator role in WebLogic Server.

7. Click **Add Conditions** to add a different group name.

The Edit Global Role - Predicate List page displays (see [Figure 14–24](#)).

**Figure 14–24 Edit Global Role Page - Predicate List**

8. Select `Group` from the **Predicate List** list and click **Next**.

The Edit Global Role - Arguments page displays (see [Figure 14–25](#)).

**Figure 14–25 Edit Global Role Page - Arguments**

9. Enter the name for the new administrator group and click **Add**.
10. Select the pre-existing administrator group and click **Remove** to delete it leaving the new one you've selected in its place.
11. Click **Finish** to save your changes.

After making this change, any members of the new group specified will be authorized to administer WebLogic Server.

### 14.3.5 Granting the WebCenter Administrator Role to a WebCenter Spaces User

WebCenter Spaces only recognizes users in the identity store that is mapped by the first authenticator. Since the WebCenter Spaces Administrator account is initially created only in the embedded LDAP server, if an external LDAP such as Oracle Internet Directory is configured as the primary authenticator for WebCenter Spaces, you must also create a user in that LDAP and grant that user the WebCenter Spaces Administrator role. For more information, see "Granting Administrator Role to a Non-Default User" in the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*.

You can grant a user the WebCenter Administrator role using Fusion Middleware Control or WLST as shown below in the sections on:

- [Granting the WebCenter Spaces Administrator Role Using Fusion Middleware Control](#)
- [Granting the WebCenter Spaces Administrator Role Using WLST](#)

#### 14.3.5.1 Granting the WebCenter Spaces Administrator Role Using Fusion Middleware Control

This section describes how to grant the WebCenter Spaces administrator role to a user account other than the default "weblogic" account.

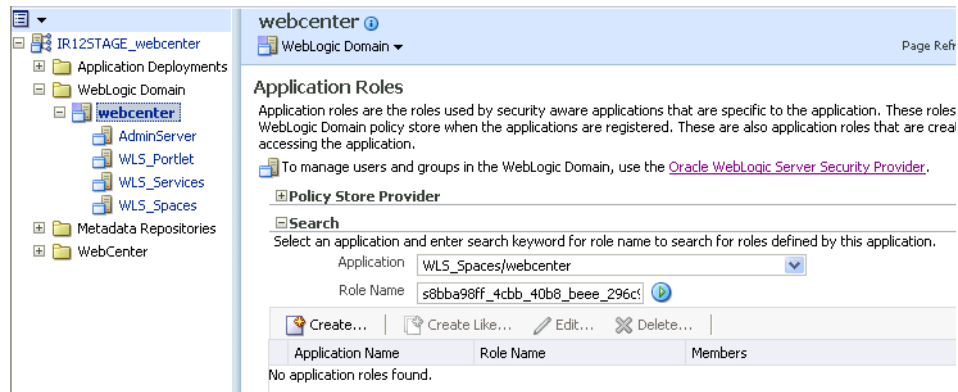
To grant the WebCenter Spaces Administrator role using Fusion Middleware Control:

1. Log into Fusion Middleware Control and select the WebLogic domain for WebCenter Spaces.

For information on logging into Fusion Middleware Control, see [Section 6, "Starting Enterprise Manager Fusion Middleware Control"](#).

- From the WebLogic Domain menu, select **Security -> Application Roles**.  
The Application Roles page displays (see [Figure 14–26](#)).

**Figure 14–26 Application Roles Page**



- Search for the Administration application role by selecting the **Application** name for WebCenter Spaces (WLS\_Spaces/webcenter), and providing the following internal identifier used by WebCenter Spaces as the **Role Name**:

s8bba98ff\_4cbb\_40b8\_beee\_296c916a23ed#-#Administrator

The search should return s8bba98ff\_4cbb\_40b8\_beee\_296c916a23ed#-#Administrator, which is the administrator role identifier.

- Click the administrator role name (s8bba98ff\_4cbb\_40b8\_beee\_296c916a23ed#-#Administrator) in the Role Name column.  
The Edit Application Role page displays (see [Figure 14–27](#)).

**Figure 14–27 Edit Application Role Page**

webcenter Logged in as weblogi  
 WebLogic Domain Page Refreshed Mar 20, 2009 11:41:14 AM PDT

Application Roles > Edit Application Role  
 Edit Application Role : s8bba98ff\_4cbb\_40b8\_... OK Cancel

**General**

Application webcenter  
 Role Name s8bba98ff\_4cbb\_40b8\_...#Administrator  
 Display Name   
 Description

**Members**  
 An application role may need to be mapped to users or groups defined in enterprise LDAP server, or the role can be mapped to other application roles.

**Roles**

+ Add Role X Delete...

| Name                                  | Type |
|---------------------------------------|------|
| No groups or application roles added. |      |

**Users**

+ Add User X Delete...

| Name      |
|-----------|
| fmwadmin  |
| psradmin1 |
| Monica    |
| weblogic  |
| orcladmin |
| psradmin2 |

5. Click **Add User**.

The Add User pop-up displays (see [Figure 14–28](#)).

**Figure 14–28 Add User Pop-up**

**Add User**

Specify criteria to search and select WebLogic users that you want to grant permissions to.

Search

Select users

| Available Users | Selected Users |
|-----------------|----------------|
|                 |                |

> Move  
 >> Move All  
 < Remove  
 << Remove All

OK Cancel

6. Use the Search function to search for the user to assign the Administrator role to.

7. Use the arrow keys to move the user from the Available Users column to the Selected Users column, and click **OK**.

8. On the Edit Application Role page, click **OK**.

9. After granting the WebCenter Spaces Administrator role to new accounts, remove this role from accounts that no longer need it or should no longer have it using the WLST `revokeAppRole` command described below. For example, if WebCenter Spaces was installed with a different administrator user name than "weblogic", the administrator role should be given to that user and should be revoked from the default "weblogic".

```
revokeAppRole(appStripe="webcenter", appRoleName="s8bba98ff_4cbb_40b8_beee_
296c916a23ed#-#Administrator",
principalClass="weblogic.security.principal.WLSUserImpl",
principalName="weblogic")
```

10. Restart the `WLS_Spaces` managed server.

When you login to WebCenter Spaces, the Administration link should appear and you should be able to perform all administrator operations. See also, [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).

### 14.3.5.2 Granting the WebCenter Spaces Administrator Role Using WLST

To grant the WebCenter Administrator role using WLST:

1. Start WLST as described in [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands"](#).
2. Connect to the WebCenter Spaces Administration Server for the target domain with the following command:

```
connect('user_name', 'password', 'host_id:port')
```

Where:

- `user_name` is the name of the user account with which to access the Administration Server (for example, `weblogic`)
  - `password` is the password with which to access the Administration Server
  - `host_id` is the host ID of the Administration Server
  - `port` is the port number of the Administration Server (for example, 7001).
3. Grant the WebCenter Spaces administrator application role to the user in Oracle Internet Directory using the `grantAppRole` command as shown below:

```
grantAppRole(appStripe="webcenter", appRoleName="s8bba98ff_4cbb_40b8_beee_
296c916a23ed#-#Administrator",
principalClass="weblogic.security.principal.WLSUserImpl", principalName="wc_
admin")
```

Where `wc_admin` is the name of the administrator account to create.

4. To test the new account, log into WebCenter Spaces using the new account name. The Administration link should appear, and you should be able to perform all administrator operations. See also, [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
5. After granting the WebCenter Spaces Administrator role to new accounts, remove this role from accounts that no longer need it or should no longer have it. For example, if WebCenter Spaces was installed with a different administrator user name than "weblogic", the administrator role should be given to that user and should be revoked from the default "weblogic".

### 14.3.6 Configuring the Discussions Server to Share the Identity Store LDAP Server

After installing Oracle Discussions, it must also be configured to use the same Identity Store as WebCenter Spaces. The Discussions server can be configured to use either the default embedded LDAP or an external LDAP server (such as Oracle Internet Directory Server) depending on the identity store used by WebCenter Spaces. The steps below describe how to configure Oracle WebCenter Discussions Server to share the same external LDAP server as the WebCenter Spaces identity store. For information on how to configure the Oracle WebCenter Discussions Server to use the same embedded LDAP server as the WebCenter Spaces identity store, see [Section 14.3.7, "Configuring the Discussions Server to Share the Identity Store Embedded LDAP Server"](#).

To configure the discussions server to share the same external LDAP server as the identity store:

1. Locate the `jive_startup.xml` file in your WebCenter installation (it can be found in `MW_HOME/user_projects/domains/<my_domain>/config/fmwconfig/servers/WLS_Services/owc_discussions_11.1.1.1.0`), and make a backup copy.
2. Change the line with the content:
 

```
<setup>true</setup>
```

 to
 

```
<setup>false</setup>
```
3. Save the file and restart the `WLS_Services` managed server.
4. Connect to the Oracle WebCenter Discussions Server administration console at:
 

```
http://host:port/owc_discussions
```

 where `host` and `port` are the host ID and port number of the `WLS_Services` managed server.
5. On the Database Settings page, choose `JNDI Datasource`, and click **Continue**.
6. On the Datasource Settings page, enter `jdbc/OWC_DiscussionsDS` as the **JNDI Datasource Name**, and click **Continue**.
7. On the User, Group and Authentication Systems page, choose `LDAP` and click **Continue**.
8. On the LDAP User System page, enter the LDAP values of the identity store and click **Continue**.
9. On the Other Settings page, check and correct the SMTP settings as appropriate for your WebCenter configuration and click **Continue**.
10. On the LDAP User Data Storage Mode page, specify a user in LDAP that should be set as the discussions server administrator (typically `orcladmin`), and click **Continue**.
 

The is the same administrator account as the one specified on the discussion connection. See also, [Section 11.1, "Setting Up Connections for the Discussions and Announcements Services"](#).
11. Restart the `WLS_Services` managed server.

## 14.3.7 Configuring the Discussions Server to Share the Identity Store Embedded LDAP Server

After installing Oracle Discussions, it must also be configured to use the same Identity Store as WebCenter Spaces. The Discussions server can be configured to use either the default embedded LDAP or an external LDAP server (such as Oracle Internet Directory Server) depending on the identity store used by WebCenter Spaces. The steps below describe how to configure the Oracle WebCenter Discussions Server to use the embedded LDAP server used by the WebCenter Spaces identity store. For information on how to configure the Oracle WebCenter Discussions Server to share the same external LDAP server as the WebCenter Spaces identity store, see [Section 14.3.6, "Configuring the Discussions Server to Share the Identity Store LDAP Server"](#).

Follow the steps below to configure the Discussions server to use the embedded LDAP server:

1. To interact with the embedded LDAP server, you first need to set up the credential for external access as the admin user ("cn=Admin") as described under **Enable External LDAP Access** in the section "Adding Users to the Embedded LDAP Using an LDIF File" in the *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter*.
2. Continue by adding users to the embedded LDAP server using an LDIF file as described under **Create an LDIF File** and **Add the Users** in the same section. Be sure to add an email address (for example, mail: john.doe@example.com) for each user added.

---

**Note:** Although you can add users to an LDAP server using the WLS Administration Console, Oracle Discussions requires that every user created has an associated email address, which can only be done through an LDIF file.

---

3. Stop the Discussions server (WLS\_Services by default).
4. Locate the `jive_startup.xml` file in your WebCenter installation (it can be found in `MW_HOME/user_projects/domains/<my_domain>/config/fmwconfig/servers/WLS_Services/owc_discussions_11.1.1.1.0`), and make a backup copy.

5. Change the line with the content:

```
<setup>>true</setup>
```

to

```
<setup>>false</setup>
```

6. Save the file and start the Discussions server (WLS\_Services by default).
7. Log in to the Discussions Server Administration Console at:

```
http://host:port/owc_discussions/admin
```

where *host* and *port* are the host ID and port number of the WLS\_Services managed server (the default port is 8890).

8. On the Installation Checklist page, click **Continue**.
9. On the Database Settings page, choose JNDI Datasource, and click **Continue**.



10. Enter `jdbc/OWC_DiscussionsDS` in the **JNDI Datasource Name** field and click **Continue**.
11. For User, Group and Authentication Systems, enter the values for the embedded LDAP system and click **Continue**.
12. For Other Settings, check that your email server settings are correct and click **Continue**.
13. For Admin Account Setup, enter the user name of the user for the Discussions (Jive) administrator.
14. Click **Continue**.

You can now log in to Oracle Discussions with any user available in the LDAP server at:

```
http://<host>:8890/owc_discussions
```

You can log in to the Oracle Discussions Admin Console at:

```
http://<host>:8890/owc_discussions/admin
```

### 14.3.8 Configuring the Oracle Content Server to Share the Identity Store LDAP Server

Oracle Content Server (OCS) must be configured to use the same identity store LDAP server as Oracle WebCenter Spaces. For more information on configuring the OCS, see the section "Configuring the Identity Store Service" in the *Oracle Fusion Middleware Security Guide*.

## 14.4 Configuring the Policy and Credential Store to Use OID

Reassociating the policy and credential store with Oracle Internet Directory (OID) consists of creating a root node in the LDAP directory, and then reassociating the policy and credential store with the OID server using Fusion Middleware Control, or from the command line using WLST as described in the following sections:

- [Creating a root Node](#)
- [Reassociating the Credential and Policy Store Using Fusion Middleware Control](#)
- [Reassociating the Credential and Policy Store Using WLST](#)

### 14.4.1 Creating a root Node

The first step in reassociating the policy and credential store with OID, is to create an LDIF file in the LDAP directory and add a root node under which all data is added. After creating the file and adding the node, continue by reassociating the store using either Fusion Middleware Control or WLST.

To create a root node:

1. Create a root node by adding the following to an LDIF file (for example, `root.ldif`) in the LDAP directory:

```
dn: cn=root_webcenter_xxxx
cn: root_webcenter_xxxx
objectclass: top
objectclass: orclcontainer
```

Where `xxxx` is a string (for example, the server name) that uniquely identifies the node.

2. Add this node to the directory by running the following LDAP command from your LDAP installation directory:

```
OID_HOME/as_1/bin/ldapadd -h ldap_host_name -p ldap_port -D cn=orcladmin -w password -v -f root.ldif
```

where:

- *OID\_HOME* is the directory in which LDAP is installed
- *ldap\_host\_name* is the host name of the OID server
- *ldap\_port* is the OID server port number
- *password* is the password with which to access the OID server

Note that each root container must have a unique name.

## 14.4.2 Reassociating the Credential and Policy Store Using Fusion Middleware Control

When initially installed, WebCenter Spaces and Enterprise Manager are already associated and deployed in the same domain.

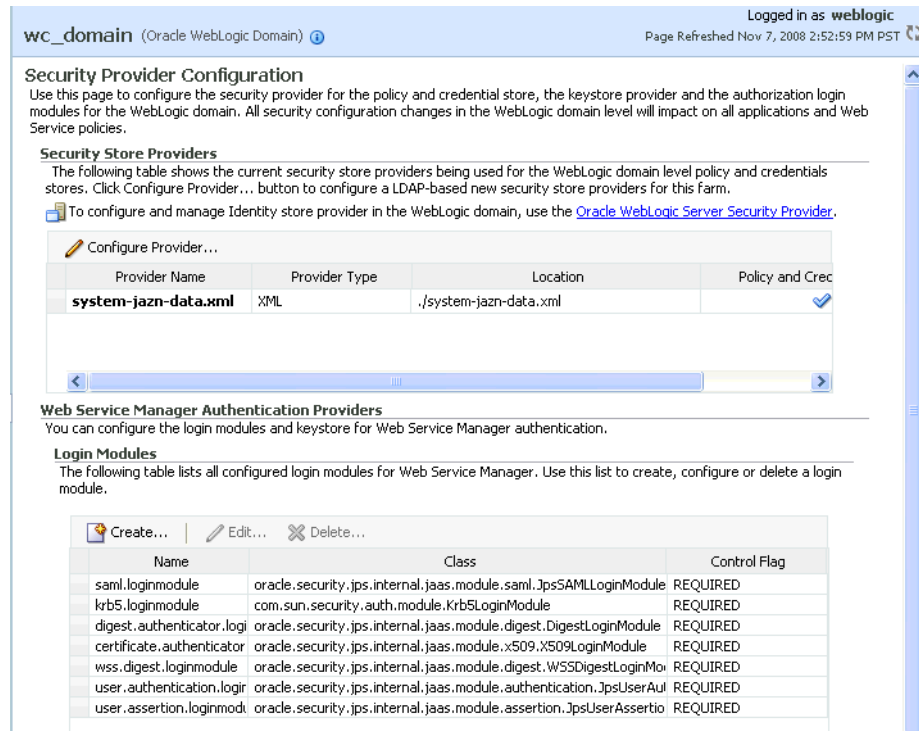
Before reassociating the policy and credential store with Oracle Internet Directory, you must first have created the root node as described in [Section 14.4.1, "Creating a root Node."](#)

To reassociate the policy and credential store with the OID server:

1. Open Fusion Middleware Control and log into your target instance.  
For information on logging into Fusion Middleware Control, see [Section 6, "Starting Enterprise Manager Fusion Middleware Control"](#).
2. In the Navigation pane, click your domain.
3. From the WebLogic Domain menu, select **Security** and then **Security Provider Configuration**.

The Security Provider Configuration page displays (see [Figure 14–29](#)).

**Figure 14–29 Security Provider Configuration Page**



This screenshot shows the Security Provider Configuration Page.

\*\*\*\*\*

4. On the Security Provider Configuration page, click **Configure...** to add the new Oracle Internet Directory provider.

The Set Security Provider page displays (see [Figure 14–30](#)).

**Figure 14–30 Set Security Provider Page**

**Information**  
All fields on this page will require a restart to take effect.

**Set Security Provider** Cancel OK  
Specify LDAP specific attributes to reassociate the policy and credential stores to the LDAP server.

**LDAP Server Details**  
Provide valid credential to connect to LDAP server. Farm uses this credential to connect to LDAP server for authentication and authorization.

LDAP Server Type: Oracle Internet Directory

\* Host:

\* Port:

User SSL to connect:

\* User DN:  Test LDAP Authentication

\* Password:

**JPS Root Node Details**  
Use this section to define provider specific configuration for this LDAP store. To specify the JPS root DN, enter the desired root name and domain name. Under Custom Properties, click Add, enter the name and desired value of the property in the resulting dialog, and click OK.

\* JPS Root DN:

\* WebLogic Domain Name: wc\_domain

Custom Properties

| Property Name                               | Value |
|---|-------|
| <span>+ Add</span> <span>✕ Delete...</span> |       |

5. Under LDAP Server Details, select **Oracle Internet Directory** as the LDAP Server Type.
6. In the **Host** and **Port** fields, enter the host name and the LDAP port for Oracle Internet Directory.
7. Set the **User DN** field to `cn=orcladmin`, and enter the associated password in the **Password** field.
8. Under JPS Root Node Details, set the JPS Root DN field to the one you added to the `root.ldif` file (for example, `cn=root_webcenter_abcd99`). Be sure to include the `cn=`.
9. Click **OK** to begin the reassociation. Restart the WebLogic server when prompted after migration.

### 14.4.3 Reassociating the Credential and Policy Store Using WLST

Before reassociating the policy and credential store with Oracle Internet Directory, you must first have created the root node as described in [Section 14.4.1, "Creating a root Node"](#).

1. Start WLST as described in [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands"](#).
2. Connect to the Administration Server for the target domain with the following command:

```
connect('username>', 'password', 'host_id:port')
```

where:

- *username* is the administrator account name used to access the Administration Server (for example, `weblogic`)
- *password* is the administrator password used to access the Administration Server (for example, `weblogic`)

- *host\_id* is the server ID of the Administration Server (for example, `example.com`)
  - *port* is the port number of the Administration Server (for example, 7001).
3. Reassociate the policy and credential store using the `reassociateSecurityStore` command:

```
reassociateSecurityStore(domain="domain_name", admin="admin_name",
password="password",
ldapurl="ldap_uri", servertype="ldap_srvr_type", jpsroot="root_webcenter_xxxx")
```

Where:

- *domain\_name* specifies the domain name where reassociation takes place.
- *admin\_name* specifies the administrator's user name on the LDAP server. The format is `cn=usrName`.
- *password* specifies the password associated with the user specified for the argument `admin`.
- *ldap\_uri* specifies the URI of the LDAP server. The format is `ldap://host:port`, if you are using a default port, or `ldaps://host:port`, if you are using a secure LDAP port. The secure port must have been configured to handle an anonymous SSL connection, and it is distinct from the default (non-secure) port.
- *ldap\_srvr\_type* specifies the kind of the target LDAP server. Valid types are `OID` (Oracle Internet Directory) or `OVD` (Oracle Virtual Directory).
- *root\_webcenter\_xxxx* specifies the root node in the target LDAP repository under which all data is migrated. Be sure to include the `cn=`. The format is `cn=nodeName`.

All arguments are required. For example:

```
reassociateSecurityStore(domain="myDomain", admin="cn=adminName",
password="myPass", ldapurl="ldaps://myhost.example.com:3060", servertype="OID",
jpsroot="cn=testNode")
```

## 14.5 Managing Users and Roles

WebCenter Spaces provides a *Users tab* from which an administrator can add users defined in the identity store, and assign roles to those users within WebCenter Spaces. For information about managing users and user roles for WebCenter Spaces, see [Chapter 19, "Managing Users and Roles for WebCenter Spaces"](#).

---

**Caution:** The "Allow Password Change" property, which specifies whether users can change their passwords within WebCenter Spaces, should be carefully controlled for corporate identity stores. WebCenter Spaces administrators can set this property from the Profile Management Settings page in WebCenter Spaces. For more information, see [Section 18.9, "Managing Personal Profiles"](#).

---

The user interface and management tools with which to manage users and user roles for custom WebCenter applications depends on what has been implemented for the particular deployment. For more information about role-mapping for ADF-security based WebCenter applications, see the section *What You May Need to Know About*

*Application Roles and Enterprise Roles in the Oracle Fusion Middleware Fusion Developer's Guide for Oracle Application Development Framework.*

## 14.6 Configuring WebCenter Applications and Components to Use SSL

This section includes the following sub-sections:

- [Securing the Browser Connection to WebCenter Spaces with SSL](#)
- [Securing the Browser Connection to a Custom WebCenter Application with SSL](#)
- [Securing the Connection from Oracle HTTP Server to WebCenter Spaces with SSL](#)
- [Securing the Browser Connection to the Wiki Service with SSL](#)
- [Securing the WebCenter Spaces Connection to Portlet Producers with SSL](#)
- [Securing the WebCenter Spaces Connection to the LDAP Identity Store](#)
- [Securing the WebCenter Spaces Connection to OCS with SSL](#)
- [Securing the WebCenter Spaces Connection to IMAP and SMTP with SSL](#)
- [Securing the WebCenter Spaces Connection to Oracle SES with SSL](#)
- [Securing the WebCenter Spaces Connection to OWLCS with SSL](#)
- [Securing the WebCenter Spaces Connection to Microsoft Live Communication Server with SSL](#)

---

---

**Note:** The following can use WS-Security with message protection, and consequently have no hard requirement for SSL:

- BPEL servers - Worklist service
  - WSRP Producers
  - Oracle WebLogic Communication Services (OWLCS) - IMP service
  - Microsoft Live Communication Server (LCS) - IMP service
  - Oracle WebCenter Discussions - Discussions and Announcements
- 
- 

### 14.6.1 Securing the Browser Connection to WebCenter Spaces with SSL

Securing the browser connection to WebCenter Spaces with SSL consists of the following steps:

- [Creating the Custom Keystore](#)
- [Configuring the Identity and Trust Keystores](#)
- [Configuring the SSL Connection](#)

#### 14.6.1.1 Creating the Custom Keystore

The first step is to generate a custom keystore for WebCenter Spaces.

To create a custom keystore:

1. Go to `JAVA_HOME/bin/` and open a command prompt.
2. Using `keytool`, generate a key pair:

```
keytool -genkeypair -keyalg RSA -dname "dname" -alias alias  
-keypass key_password -keystore keystore -storepass keystore_password
```

```
-validity days_valid
```

Where:

- *dname* is the DN (distinguished name) to use (for example, `cn=customidentity,dc=example,dc=com`)
- *alias* is the alias to use (for example, `webcenter_wls`)
- *key\_password* is the password for the new public key, (for example, `welcome1`)
- *keystore* is the keystore name, (for example, `webcenter_wls.jks`)
- *keystore\_password* is the keystore password, (for example, `welcome1`)
- *days\_valid* is the number of days for which the key password is valid (for example, `360`).

---



---

**Note:** You must use the `-keyalg` parameter and specify `RSA` as its value as shown above as the default algorithm (DSA) used by `keytool` for generating the key is incompatible with Oracle WebServices Security Manager requirements.

---



---

3. Export the certificate containing the public key so WebCenter Spaces clients can import it into their trust store:

```
keytool -exportcert -v -alias alias -keystore keystore
-storepass keystore_password -rfc -file certificate_file
```

Where:

- *alias* is the WebCenter Spaces alias (for example, `webcenter_wls`)
- *keystore* is the keystore name, (for example, `webcenter_wls.jks`)
- *keystore\_password* is the keystore password, (for example, `welcome1`)
- *certificate\_file* is the file name for the certificate to export the key to (for example, `webcenter_wls.cer`)

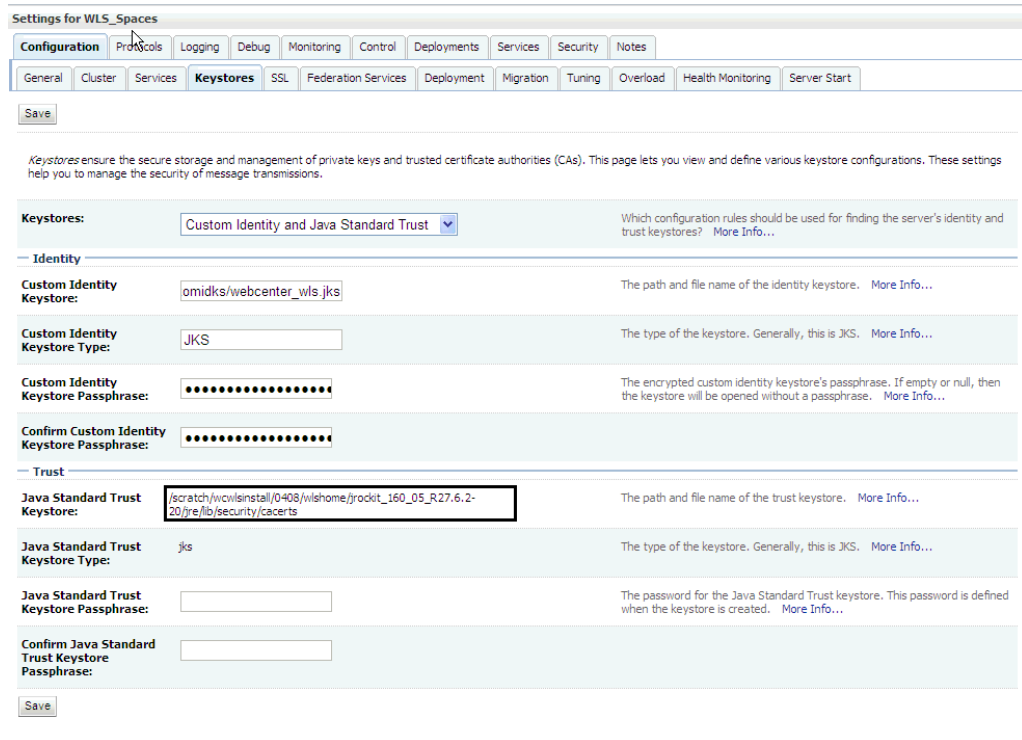
4. Determine the trust store to use:

Since you are using a self-signed certificate, you must update it as a trusted certificate in the server trust store. To do this, you must determine your trust store by going to the server:

- a. Log into the WLS Administration Console.
- b. In the Domain Structure pane, expand Environments and click `Servers`.
- c. In the list of servers, click `WLS_Spaces`.
- d. Open the Configuration tab, and the Keystores subtab.

The Keystores Settings pane displays (see [Figure 14-31](#)).

**Figure 14–31 Keystores Settings Pane**



- e. Note down the location of the server in the **Java Standard Trust Keystore** field (shown in Figure 14–31).

Note that the `cacerts` file may be "read only", in which case you will need to change its permissions so that it's writable.

5. Import the self-signed certificate generated above in this trust store:

```
keytool -importcert -trustcacerts -alias alias -file certificate_file
-keystore cacerts -storepass changeit
```

Where:

- `alias` is the WebCenter Spaces alias (for example, `webcenter_wls`)
- `certificate_file` is the file name for the certificate to export the key to (for example, `webcenter_wls.cer`)

### 14.6.1.2 Configuring the Identity and Trust Keystores

The next step is to configure the identity and trust keystores on the WebCenter Spaces server.

To configure the identity and trust keystores:

1. Log in to the WLS Administration Console.



For information on logging into the WLS Administration Console, see [Section 1.12.2, "Oracle WebLogic Server Administration Console"](#).

- In the Domain Structure pane, expand **Environment** and click **Servers**.  
The Summary of Servers pane displays (see [Figure 14–32](#)).

**Figure 14–32 Summary of Servers Pane**

**Summary of Servers**

**Configuration** Control

A server is an instance of WebLogic Server that runs in its own Java Virtual Machine (JVM) and has its own configuration.  
This page summarizes each server that has been configured in the current WebLogic Server domain.

[Customize this table](#)

**Servers (Filtered - More Columns Exist)**

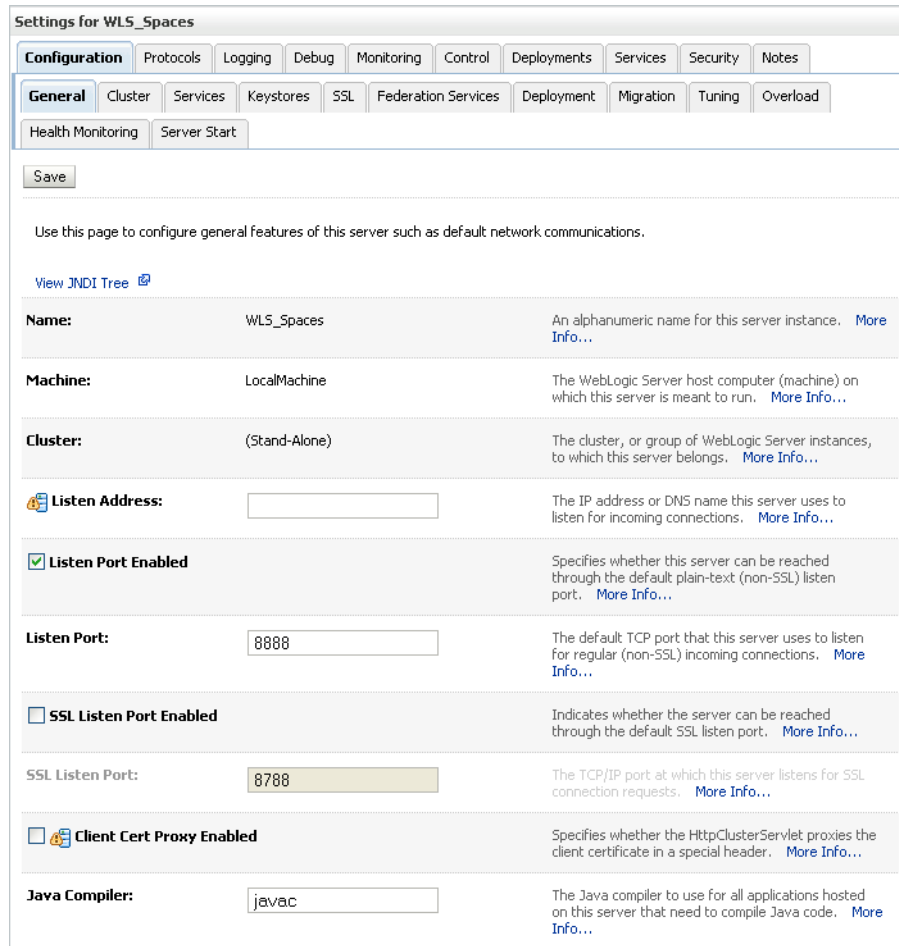
New Clone Delete Showing 1 to 4 of 4 Previous | Next

| <input type="checkbox"/> | Name               | Cluster | Machine      | State    | Health | Listen Port |
|--------------------------|--------------------|---------|--------------|----------|--------|-------------|
| <input type="checkbox"/> | AdminServer(admin) |         |              | RUNNING  | OK     | 7001        |
| <input type="checkbox"/> | WLS_Custom         |         | LocalMachine | SHUTDOWN |        | 8887        |
| <input type="checkbox"/> | WLS_Portlet        |         | LocalMachine | RUNNING  | OK     | 8889        |
| <input type="checkbox"/> | WLS_Spaces         |         | LocalMachine | RUNNING  | OK     | 8888        |

New Clone Delete Showing 1 to 4 of 4 Previous | Next

- Click the WebCenter Spaces server (`WLS_Spaces`) to configure the identity and trust keystores.  
The Settings pane for the WebCenter Spaces server displays (see [Figure 14–33](#)).

**Figure 14–33 Settings Pane for WebCenter Spaces Server**



This screenshot shows the WLS Administration Console's Settings panel for the WebCenter Spaces server.

\*\*\*\*\*

4. Open the **Configuration** tab, and then the **Keystores** subtab.

The Keystores pane displays (see [Figure 14–34](#)).

Figure 14–34 Keystores Pane

Settings for WLS\_Spaces

Configuration Protocols Logging Debug Monitoring Control Deployments Services Security Notes

General Cluster Services **Keystores** SSL Federation Services Deployment Migration Tuning Overload

Health Monitoring Server Start

Save

Keystores ensure the secure storage and management of private keys and trusted certificate authorities (CAs). This page lets you view and define various keystore configurations. These settings help you to manage the security of message transmissions.

**Keystores:** Custom Identity and Java Standard Trust  Which configuration rules should be used for finding the server's identity and trust keystores? [More Info...](#)

**Identity**

**Custom Identity Keystore:**  The path and file name of the identity keystore. [More Info...](#)

**Custom Identity Keystore Type:**  The type of the keystore. Generally, this is JKS. [More Info...](#)

**Custom Identity Keystore Passphrase:**  The encrypted custom identity keystore's passphrase. If empty or null, then the keystore will be opened without a passphrase. [More Info...](#)

**Confirm Custom Identity Keystore Passphrase:**

**Trust**

**Java Standard Trust Keystore:** /u01/app/oracle/product/IR11/fmwhome/jdk160\_05\_R27.6.1-25/jre/lib/security/cacerts The path and file name of the trust keystore. [More Info...](#)

**Java Standard Trust Keystore Type:** jks The type of the keystore. Generally, this is JKS. [More Info...](#)

**Java Standard Trust Keystore Passphrase:**  The password for the Java Standard Trust keystore. This password is defined when the keystore is created. [More Info...](#)

**Confirm Java Standard Trust Keystore Passphrase:**

Save

5. For **Keystores**, select **Custom Identity** and click **Save**.
6. Enter the path of the custom identity store in the **Java Standard Trust Keystore** field.
7. Enter **jksc** as the **Java Standard Trust Keystore Type**.
8. Enter and confirm the **Java Standard Trust Keystore**.
9. Click **Save** to save your entries.
10. Open the **SSL** tab.
11. Enter the **Private Key Alias**.
12. Enter the **Private Key Passphrase**.
13. Click **Save** to save your entries.

### 14.6.1.3 Configuring the SSL Connection

To configure the SSL connection:

1. On the Settings pane for the WebCenter Spaces server, open the **Configuration** tab and then the **General** subtab.

The General Configuration pane displays (see [Figure 14–35](#)).

**Figure 14–35 General Configuration Pane**

**Settings for WLS\_Spaces**

Configuration Protocols Logging Debug Monitoring Control Deployments Services Security Notes

General Cluster Services Keystores SSL Federation Services Deployment Migration Tuning Overload

Health Monitoring Server Start

Save

Use this page to configure general features of this server such as default network communications.

[View JNDI Tree](#)

|  |                                    |  |
|--|------------------------------------|--|
| <b>Name:</b>   | WLS_Spaces                         | An alphanumeric name for this server instance. <a href="#">More Info...</a>  |
| <b>Machine:</b>  | LocalMachine                       | The WebLogic Server host computer (machine) on which this server is meant to run. <a href="#">More Info...</a>                   |
| <b>Cluster:</b>  | (Stand-Alone)                      | The cluster, or group of WebLogic Server instances, to which this server belongs. <a href="#">More Info...</a>                   |
| <b>Listen Address:</b>   | <input type="text"/>               | The IP address or DNS name this server uses to listen for incoming connections. <a href="#">More Info...</a>                     |
| <input type="checkbox"/> <b>Listen Port Enabled</b>                |                                    | Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. <a href="#">More Info...</a>  |
| <b>Listen Port:</b>  | <input type="text" value="8888"/>  | The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. <a href="#">More Info...</a>    |
| <input checked="" type="checkbox"/> <b>SSL Listen Port Enabled</b> |                                    | Indicates whether the server can be reached through the default SSL listen port. <a href="#">More Info...</a>                    |
| <b>SSL Listen Port:</b>  | <input type="text" value="8788"/>  | The TCP/IP port at which this server listens for SSL connection requests. <a href="#">More Info...</a>                           |
| <input type="checkbox"/> <b>Client Cert Proxy Enabled</b>          |                                    | Specifies whether the HttpClusterServlet proxies the client certificate in a special header. <a href="#">More Info...</a>        |
| <b>Java Compiler:</b>  | <input type="text" value="javac"/> | The Java compiler to use for all applications hosted on this server that need to compile Java code. <a href="#">More Info...</a> |

[Advanced](#)

Save

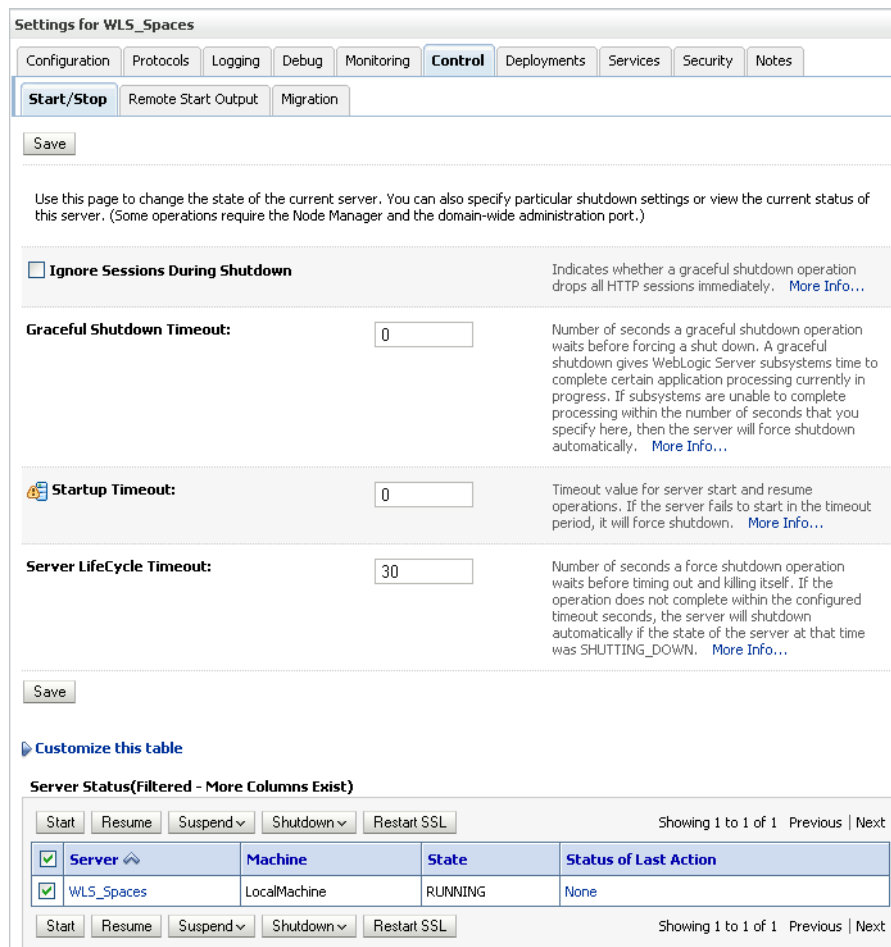
2. Check **SSL Listen Port Enabled**.
3. Enter an **SSL Listen Port** number and click **Save**.
4. Open the **SSL** subtab and expand the **Advanced** options at the bottom of the page. The **SSL** advanced options are displayed (see [Figure 14–36](#)).

**Figure 14–36 Advanced SSL Configuration Settings**

| Advanced  |                             |  |
|---|-----------------------------|--|
| <b>Hostname Verification:</b>   | BEA Hostname Verifier       | Specifies whether to ignore the installed implementation of the <code>weblogic.security.SSL.HostnameVerifier</code> interface (when this server is acting as a client to another application server). <a href="#">More Info...</a>   |
| <b>Custom Hostname Verifier:</b>  |                             | The name of the class that implements the <code>weblogic.security.SSL.HostnameVerifier</code> interface. <a href="#">More Info...</a>  |
| <b>Export Key Lifespan:</b>   | 500                         | Indicates the number of times WebLogic Server can use an exportable key between a domestic server and an exportable client before generating a new key. The more secure you want WebLogic Server to be, the fewer times the key should be used before generating a new key. <a href="#">More Info...</a>                     |
| <input type="checkbox"/> <b>Use Server Certs</b>                        |                             | Sets whether the client should use the server certificates/key as the client identity when initiating a connection over https. <a href="#">More Info...</a>  |
| <b>Two Way Client Cert Behavior:</b>                                    | Client Certs Not Requested  | The form of SSL that should be used. <a href="#">More Info...</a>  |
| <b>Cert Authenticator:</b>  |                             | The name of the Java class that implements the <code>weblogic.security.ad.CertAuthenticator</code> class, which is deprecated in this release of WebLogic Server. This field is for Compatibility security only, and is only used when the Realm Adapter Authentication provider is configured. <a href="#">More Info...</a> |
| <input checked="" type="checkbox"/> <b>SSLRejection Logging Enabled</b> |                             | Indicates whether warning messages are logged in the server log when SSL connections are rejected. <a href="#">More Info...</a>  |
| <input type="checkbox"/> <b>Allow Unencrypted Null Cipher</b>           |                             | Test if the <code>AllowUnEncryptedNullCipher</code> is enabled. <a href="#">More Info...</a>   |
| <b>Inbound Certificate Validation:</b>                                  | Builtin SSL Validation Only | Indicates the client certificate validation rules for inbound SSL. <a href="#">More Info...</a>  |
| <b>Outbound Certificate Validation:</b>                                 | Builtin SSL Validation Only | Indicates the server certificate validation rules for outbound SSL. <a href="#">More Info...</a>   |
| <input type="button" value="Save"/>                                     |                             |  |

5. Set the **Two Way Client Cert Behavior** option to `Client Certs Not Requested` and click **Save**.
6. Open the Control tab.  
The Control Settings pane displays (see [Figure 14–37](#)).

**Figure 14–37 Control Settings Pane**



7. Click **Restart SSL**.
8. Restart the WebLogic Server and open the SSL WebCenter Spaces URL.
9. Accept the certificate for the session and log in.

## 14.6.2 Securing the Browser Connection to a Custom WebCenter Application with SSL

Securing the browser connection to a custom WebCenter application uses the same configuration steps as for securing the browser connection to WebCenter Spaces. The only difference is that the configuration occurs on the managed server that is hosting the custom WebCenter application deployment rather than the `WLS_Spaces` server. For more information, see [Section 14.6.1, "Securing the Browser Connection to WebCenter Spaces with SSL"](#).

## 14.6.3 Securing the Connection from Oracle HTTP Server to WebCenter Spaces with SSL

Securing the connection between the Oracle HTTP Server (OHS) and WebCenter Spaces consists of these steps:

- [Configure the Identity and Trust Keystores](#)
- [Configure the SSL Connection](#)

- [Install OHS](#)
- [Wire WebCenter Spaces Ports to OHS](#)
- [Configure the SSL Certificates](#)

### Configure the Identity and Trust Keystores

For instructions on how to configure the Identity and Trust keystores, see [Section 14.6.1, "Securing the Browser Connection to WebCenter Spaces with SSL"](#).

### Configure the SSL Connection

1. On the Settings pane for the WebCenter Spaces server, open the Configuration tab and then the General subtab.

The General Configuration pane displays (see [Figure 14–38](#)).

**Figure 14–38** General Configuration Pane

Settings for WLS\_Spaces

Configuration Protocols Logging Debug Monitoring Control Deployments Services Security Notes

General Cluster Services Keystores SSL Federation Services Deployment Migration Tuning Overload

Health Monitoring Server Start

Save

Use this page to configure general features of this server such as default network communications.

[View JNDI Tree](#)

|  |                                    |  |
|--|------------------------------------|--|
| <b>Name:</b>   | WLS_Spaces                         | An alphanumeric name for this server instance. <a href="#">More Info...</a>  |
| <b>Machine:</b>  | LocalMachine                       | The WebLogic Server host computer (machine) on which this server is meant to run. <a href="#">More Info...</a>                   |
| <b>Cluster:</b>  | (Stand-Alone)                      | The cluster, or group of WebLogic Server instances, to which this server belongs. <a href="#">More Info...</a>                   |
| <b>Listen Address:</b>   | <input type="text"/>               | The IP address or DNS name this server uses to listen for incoming connections. <a href="#">More Info...</a>                     |
| <input type="checkbox"/> <b>Listen Port Enabled</b>                |                                    | Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. <a href="#">More Info...</a>  |
| <b>Listen Port:</b>  | <input type="text" value="8888"/>  | The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. <a href="#">More Info...</a>    |
| <input checked="" type="checkbox"/> <b>SSL Listen Port Enabled</b> |                                    | Indicates whether the server can be reached through the default SSL listen port. <a href="#">More Info...</a>                    |
| <b>SSL Listen Port:</b>  | <input type="text" value="8788"/>  | The TCP/IP port at which this server listens for SSL connection requests. <a href="#">More Info...</a>                           |
| <input type="checkbox"/> <b>Client Cert Proxy Enabled</b>          |                                    | Specifies whether the HttpClusterServlet proxies the client certificate in a special header. <a href="#">More Info...</a>        |
| <b>Java Compiler:</b>  | <input type="text" value="javac"/> | The Java compiler to use for all applications hosted on this server that need to compile Java code. <a href="#">More Info...</a> |

[Advanced](#)

Save

2. Check **SSL Listen Port Enabled**.
3. Enter an **SSL Listen Port** number and click **Save**.

4. On the **Configuration** tab, open the **SSL** subtab, and then expand the **Advanced** options at the bottom of the page.

The SSL advanced options are displayed (see [Figure 14–39](#)).

**Figure 14–39 Advanced SSL Configuration Settings**

The screenshot shows the 'Advanced' configuration tab for SSL. It contains several settings:

- Hostname Verification:** Set to 'BEA Hostname Verifier'. Description: Specifies whether to ignore the installed implementation of the `weblogic.security.SSL.HostnameVerifier` interface (when this server is acting as a client to another application server). [More Info...](#)
- Custom Hostname Verifier:** An empty text field. Description: The name of the class that implements the `weblogic.security.SSL.HostnameVerifier` interface. [More Info...](#)
- Export Key Lifespan:** Set to '500'. Description: Indicates the number of times WebLogic Server can use an exportable key between a domestic server and an exportable client before generating a new key. The more secure you want WebLogic Server to be, the fewer times the key should be used before generating a new key. [More Info...](#)
- Use Server Certs:** An unchecked checkbox. Description: Sets whether the client should use the server certificates/key as the client identity when initiating a connection over https. [More Info...](#)
- Two Way Client Cert Behavior:** Set to 'Client Certs Not Requested'. Description: The form of SSL that should be used. [More Info...](#)
- Cert Authenticator:** An empty text field. Description: The name of the Java class that implements the `weblogic.security.ac.CertAuthenticator` class, which is deprecated in this release of WebLogic Server. This field is for Compatibility security only, and is only used when the Realm Adapter Authentication provider is configured. [More Info...](#)
- SSL Rejection Logging Enabled:** A checked checkbox. Description: Indicates whether warning messages are logged in the server log when SSL connections are rejected. [More Info...](#)
- Allow Unencrypted Null Cipher:** An unchecked checkbox. Description: Test if the `AllowUnEncryptedNullCipher` is enabled. [More Info...](#)
- Inbound Certificate Validation:** Set to 'Builtin SSL Validation Only'. Description: Indicates the client certificate validation rules for inbound SSL. [More Info...](#)
- Outbound Certificate Validation:** Set to 'Builtin SSL Validation Only'. Description: Indicates the server certificate validation rules for outbound SSL. [More Info...](#)

A 'Save' button is located at the bottom left of the configuration area.

5. Set the **Two Way Client Cert Behavior** option to **Client Certs Not Requested** and click **Save**.
6. Open the **Control** tab on the Settings pane, and select the **Start/Stop** subtab.
7. Click **Restart SSL**.
8. Open the SSL WebCenter Spaces URL.
9. Accept the certificate for the session and log in.
10. In the WSL Administration Console, click **View Changes and Restarts** on the Change Center pane and restart any affected servers or components.

### Install OHS

1. Install the WebTier.
  - Do not select WebCache; only select the HTTP Server.
  - Uncheck the checkbox to associate a WebLogic server during install.



2. Navigate to the `OHS_HOME/instances/instance1/bin` directory and start OHS using the following command:

```
./opmnctl startall
```

3. Check the status of OHS using the following command:

```
./opmnctl status -l
```

### Wire WebCenter Spaces Ports to OHS

1. Open the file `OHS_HOME/instances/instance1/config/OHS/ohs1/mod_wl.conf`
2. Add the following entry to `mod_wl.conf` to make WebCenter Spaces work with OHS:

```
<IfModule mod_weblogic.c>
    WebLogicHost host_id
    WebLogicPort port
    Debug OFF
    WLLogFile /tmp/ohs.log
    MatchExpression *.jsp
</IfModule>

<Location />
    SetHandler weblogic-handler
</Location>
```

Replacing *host\_id* and *port* with the WebCenter Spaces server ID and port number.

3. Open the file `OHS_HOME/instances/instance1/config/OHS/ohs1/mod_ssl.conf`.
4. Add the following entry to `mod_ssl.conf` to make WebCenter Spaces run on the OHS SSL port:

```
<IfModule mod_weblogic.c>
    WebLogicHost host_id
    WebLogicPort port
    WLLogFile /tmp/ohs_ssl.log
    Debug OFF
    DebugConfigInfo ON
    SecureProxy ON
    MatchExpression *.jsp
    WLSslWallet SSL_wallet
</IfModule>

<Location />
    SetHandler weblogic-handler
</Location>
```

Replacing *host\_id* and *port* with the WebCenter SSL server ID and port number, and *SSL\_wallet* with the path to the WebLogic SSL wallet (for example, `OHS_HOME>/oracle/product/11.1.1/as_1/instances/instance1/config/OHS/ohs1/keystores/default`).

5. Go to `OHS_HOME>/instances/instance1/bin` and start and check the status of OHS using the following commands:

```
./opmnctl stopall
```

```
./opmnctl startall
./opmnctl status -l
```

### Configure the SSL Certificates

1. For OHS to trust WebCenter's certificate, the WLS\_Spaces certificate must be imported into the OHS trust store. Export the certificate from the WLS\_Spaces identity keystore:

```
keytool -exportcert -v -alias webcenter_wls -keystore webcenter_wls.jks
-storepass <password> -rfc -file webcenter_wls.cer
```

2. Import the certificate into the wallet on the OHS side using orapki:

```
orapki wallet add -wallet . -trusted_cert -cert webcenter_wls.cer -auto_login_
only
```

3. For WebCenter to trust OHS certificates, export the user certificate from OHS wallet and import it as a trusted certificate in the WebLogic trust store.

```
orapki wallet export -wallet . -cert cert.txt -dn 'CN=\"Self-signed
Certificate for ohs1
\", OU=EXAMPLEORGUNIT, O=EXAMPLEORG, L=EXAMPLELOCATION, ST=CA, C=US'
```

4. Import the above certificate into the WLS\_Spaces managed server trust store available in /scratch/wcwlinstall/0408/wlshome/jrockit\_160\_05\_R27.6.2-20/jre/lib/security/cacerts:

```
keytool -file cert.txt -importcert -trustcacerts -alias ohs_cert -keystore
cacerts -storepass changeit
```

5. Restart OHS and the WLS\_Spaces server.

You should now be able to access the SSL OHS, as well as the non-SSL OHS.

## 14.6.4 Securing the Browser Connection to the Wiki Service with SSL

As with securing the browser connection to WebCenter Spaces, securing the Wiki service connection with SSL consists of two steps:

- [Configure the identity and trust keystores](#)
- [Configure the SSL connection](#)

### Configure the identity and trust keystores

1. Log in to the WLS Administration Console.

For information on logging into the WLS Administration Console, see [Section 1.12.2, "Oracle WebLogic Server Administration Console"](#).

2. In the Domain Structure pane, expand **Environment** and click **Servers**.

The Summary of Servers pane displays (see [Figure 14-40](#)).

**Figure 14–40 Summary of Servers Pane**

**Configuration** Control

A server is an instance of WebLogic Server that runs in its own Java Virtual Machine (JVM) and has its own configuration.  
This page summarizes each server that has been configured in the current WebLogic Server domain.

[Customize this table](#)

**Servers (Filtered - More Columns Exist)**

New Clone Delete Showing 1 to 4 of 4 Previous | Next

| <input type="checkbox"/> | Name ↕             | Cluster | Machine | State   | Health | Listen Port |
|--------------------------|--------------------|---------|---------|---------|--------|-------------|
| <input type="checkbox"/> | AdminServer(admin) |         |         | RUNNING | ✔ OK   | 7001        |
| <input type="checkbox"/> | WLS_Portlet        |         |         | RUNNING | ✔ OK   | 8889        |
| <input type="checkbox"/> | WLS_Services       |         |         | RUNNING | ✔ OK   | 8890        |
| <input type="checkbox"/> | WLS_Spaces         |         |         | RUNNING | ✔ OK   | 8888        |

New Clone Delete Showing 1 to 4 of 4 Previous | Next

3. Click the Services server (WLS\_Services) to configure the identity and trust keystores.

The Settings pane for the services server displays (see [Figure 14–41](#)).

**Figure 14–41 Settings Pane for Services Server**

The screenshot shows the 'Configuration' tab selected, with sub-tabs for 'General', 'Cluster', 'Services', 'Keystores', 'SSL', 'Federation Services', 'Deployment', 'Migration', 'Tuning', and 'Overload'. The 'General' sub-tab is active, showing a 'Save' button and a description: 'Use this page to configure general features of this server such as default network communications.' Below this is a 'View JNDI Tree' link. The main configuration area contains several rows, each with a label, a value field, and a description with a 'More Info...' link:

- Name:** WLS\_Services. Description: An alphanumeric name for this server instance.
- Machine:** (None). Description: The WebLogic Server host computer (machine) on which this server is meant to run.
- Cluster:** (Stand-Alone). Description: The cluster, or group of WebLogic Server instances, to which this server belongs.
- Listen Address:** [Empty text box]. Description: The IP address or DNS name this server uses to listen for incoming connections.
- Listen Port Enabled:** . Description: Specifies whether this server can be reached through the default plain-text (non-SSL) listen port.
- Listen Port:** 8890. Description: The default TCP port that this server uses to listen for regular (non-SSL) incoming connections.
- SSL Listen Port Enabled:** . Description: Indicates whether the server can be reached through the default SSL listen port.
- SSL Listen Port:** 8790. Description: The TCP/IP port at which this server listens for SSL connection requests.
- Client Cert Proxy Enabled:** . Description: Specifies whether the HttpClusterServlet proxies the client certificate in a special header.
- Java Compiler:** javac. Description: The Java compiler to use for all applications hosted on this server that need to compile Java code.

At the bottom, there is an 'Advanced' section with a 'Save' button.

4. Open the **Configuration** tab, and then the **Keystores** subtab. The Keystores pane displays (see [Figure 14–42](#)).

Figure 14–42 Keystores Pane

Settings for WLS\_Services

Configuration Protocols Logging Debug Monitoring Control Deployments Services Security Notes

General Cluster Services **Keystores** SSL Federation Services Deployment Migration Tuning Overload

Health Monitoring Server Start

Save

Keystores ensure the secure storage and management of private keys and trusted certificate authorities (CAs). This page lets you view and define various keystore configurations. These settings help you to manage the security of message transmissions.

Keystores: Custom Identity and Java Standard Trust Which configuration rules should be used for finding the server's identity and trust keystores? [More Info...](#)

— Identity —

Custom Identity Keystore:  The path and file name of the identity keystore. [More Info...](#)

Custom Identity Keystore Type:  The type of the keystore. Generally, this is JKS. [More Info...](#)

Custom Identity Keystore Passphrase:  The encrypted custom identity keystore's passphrase. If empty or null, then the keystore will be opened without a passphrase. [More Info...](#)

Confirm Custom Identity Keystore Passphrase:

— Trust —

Java Standard Trust Keystore:  /u01/app/oracle/product/IR13/fmwhome/rockit\_160\_05\_R27.6.2-20/jre/lib/security/cacerts The path and file name of the trust keystore. [More Info...](#)

Java Standard Trust Keystore Type:  jks The type of the keystore. Generally, this is JKS. [More Info...](#)

Java Standard Trust Keystore Passphrase:  The password for the Java Standard Trust keystore. This password is defined when the keystore is created. [More Info...](#)

Confirm Java Standard Trust Keystore Passphrase:

Save

5. For Keystores, select **Custom Identity and Java Standard Trust** and click **Save**.
6. Open the Control tab.  
The Control Settings pane displays (see [Figure 14–43](#)).

**Figure 14–43 Control Settings Pane**

**Settings for WLS\_Services**

Configuration Protocols Logging Debug Monitoring **Control** Deployments Services Security Notes

Start/Stop Remote Start Output Migration

Save

Use this page to change the state of the current server. You can also specify particular shutdown settings or view the current status of this server. (Some operations require the Node Manager and the domain-wide administration port.)

**Ignore Sessions During Shutdown** Indicates whether a graceful shutdown operation drops all HTTP sessions immediately. [More Info...](#)

**Graceful Shutdown Timeout:**  Number of seconds a graceful shutdown operation waits before forcing a shut down. A graceful shutdown gives WebLogic Server subsystems time to complete certain application processing currently in progress. If subsystems are unable to complete processing within the number of seconds that you specify here, then the server will force shutdown automatically. [More Info...](#)

**Startup Timeout:**  Timeout value for server start and resume operations. If the server fails to start in the timeout period, it will force shutdown. [More Info...](#)

**Server LifeCycle Timeout:**  Number of seconds a force shutdown operation waits before timing out and killing itself. If the operation does not complete within the configured timeout seconds, the server will shutdown automatically if the state of the server at that time was SHUTTING\_DOWN. [More Info...](#)

Save

[Customize this table](#)

**Server Status(Filtered - More Columns Exist)**

Start Resume Suspend Shutdown Restart SSL Showing 1 to 1 of 1 Previous | Next

| <input checked="" type="checkbox"/> | Server       | Machine | State   | Status of Last Action |
|-------------------------------------|--------------|---------|---------|-----------------------|
| <input checked="" type="checkbox"/> | WLS_Services |         | RUNNING | None                  |

Start Resume Suspend Shutdown Restart SSL Showing 1 to 1 of 1 Previous | Next

7. Click **Restart SSL**.

**Configure the SSL connection**

1. On the Settings pane for the Services server, open the Configuration tab and then the General subtab.

The General Configuration pane displays (see [Figure 14–44](#)).

Figure 14–44 General Configuration Pane

Settings for WLS\_Services

Configuration Protocols Logging Debug Monitoring Control Deployments Services Security Notes

General Cluster Services Keystores SSL Federation Services Deployment Migration Tuning Overload

Health Monitoring Server Start

Save

Use this page to configure general features of this server such as default network communications.

[View JNDI Tree](#)

|  |                                    |  |
|--|------------------------------------|--|
| <b>Name:</b>   | WLS_Spaces                         | An alphanumeric name for this server instance. <a href="#">More Info...</a>  |
| <b>Machine:</b>  | LocalMachine                       | The WebLogic Server host computer (machine) on which this server is meant to run. <a href="#">More Info...</a>                   |
| <b>Cluster:</b>  | (Stand-Alone)                      | The cluster, or group of WebLogic Server instances, to which this server belongs. <a href="#">More Info...</a>                   |
| <b>Listen Address:</b>   | <input type="text"/>               | The IP address or DNS name this server uses to listen for incoming connections. <a href="#">More Info...</a>                     |
| <input type="checkbox"/> <b>Listen Port Enabled</b>                |                                    | Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. <a href="#">More Info...</a>  |
| <b>Listen Port:</b>  | <input type="text" value="8888"/>  | The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. <a href="#">More Info...</a>    |
| <input checked="" type="checkbox"/> <b>SSL Listen Port Enabled</b> |                                    | Indicates whether the server can be reached through the default SSL listen port. <a href="#">More Info...</a>                    |
| <b>SSL Listen Port:</b>  | <input type="text" value="8788"/>  | The TCP/IP port at which this server listens for SSL connection requests. <a href="#">More Info...</a>                           |
| <input type="checkbox"/> <b>Client Cert Proxy Enabled</b>          |                                    | Specifies whether the HttpClusterServlet proxies the client certificate in a special header. <a href="#">More Info...</a>        |
| <b>Java Compiler:</b>  | <input type="text" value="javac"/> | The Java compiler to use for all applications hosted on this server that need to compile Java code. <a href="#">More Info...</a> |

Advanced

Save

2. Check **SSL Listen Port Enabled**.
3. Enter an **SSL Listen Port** number and click **Save**.
4. On the **Configuration** tab, open the **SSL** subtab, and then expand the **Advanced** options at the bottom of the page.

The SSL advanced options are displayed (see [Figure 14–45](#)).

**Figure 14–45 Advanced SSL Configuration Settings**

| Advanced  |                             |  |
|---|-----------------------------|--|
| <b>Hostname Verification:</b>   | BEA Hostname Verifier       | Specifies whether to ignore the installed implementation of the <code>weblogic.security.SSL.HostnameVerifier</code> interface (when this server is acting as a client to another application server). <a href="#">More Info...</a>   |
| <b>Custom Hostname Verifier:</b>  |                             | The name of the class that implements the <code>weblogic.security.SSL.HostnameVerifier</code> interface. <a href="#">More Info...</a>  |
| <b>Export Key Lifespan:</b>   | 500                         | Indicates the number of times WebLogic Server can use an exportable key between a domestic server and an exportable client before generating a new key. The more secure you want WebLogic Server to be, the fewer times the key should be used before generating a new key. <a href="#">More Info...</a>                     |
| <input type="checkbox"/> <b>Use Server Certs</b>                        |                             | Sets whether the client should use the server certificates/key as the client identity when initiating a connection over https. <a href="#">More Info...</a>  |
| <b>Two Way Client Cert Behavior:</b>                                    | Client Certs Not Requested  | The form of SSL that should be used. <a href="#">More Info...</a>  |
| <b>Cert Authenticator:</b>  |                             | The name of the Java class that implements the <code>weblogic.security.ac.CertAuthenticator</code> class, which is deprecated in this release of WebLogic Server. This field is for Compatibility security only, and is only used when the Realm Adapter Authentication provider is configured. <a href="#">More Info...</a> |
| <input checked="" type="checkbox"/> <b>SSLRejection Logging Enabled</b> |                             | Indicates whether warning messages are logged in the server log when SSL connections are rejected. <a href="#">More Info...</a>  |
| <input type="checkbox"/> <b>Allow Unencrypted Null Cipher</b>           |                             | Test if the <code>AllowUnencryptedNullCipher</code> is enabled. <a href="#">More Info...</a>   |
| <b>Inbound Certificate Validation:</b>                                  | Builtin SSL Validation Only | Indicates the client certificate validation rules for inbound SSL. <a href="#">More Info...</a>  |
| <b>Outbound Certificate Validation:</b>                                 | Builtin SSL Validation Only | Indicates the server certificate validation rules for outbound SSL. <a href="#">More Info...</a>   |
| <input type="button" value="Save"/>                                     |                             |  |

5. Set the **Two Way Client Cert Behavior** option to **Client Certs Not Requested** and click **Save**.
6. Restart the `WLS_Services` server and open the SSL Wiki URL at `https://host:port/owc_wiki`.
7. Accept the certificate for the session and log in.

### 14.6.5 Securing the WebCenter Spaces Connection to Portlet Producers with SSL

Securing the connection to WSRP and PDK-Java portlet producers with SSL consists of the following steps:

- [Configure the identity and trust keystores](#)
- [Configure the SSL connection](#)
- [Register the SSL-enabled WSRP producer and run the portlets](#)
- [Register the SSL-enabled PDK-Java Producer and run the portlets](#)

#### Configure the identity and trust keystores

1. Log in to the WLS Administration Console.



For information on logging into the WLS Administration Console, see [Section 1.12.2, "Oracle WebLogic Server Administration Console"](#).

- In the Domain Structure pane, expand **Environment** and click **Servers**.  
The Summary of Servers pane displays (see [Figure 14-46](#)).

**Figure 14-46 Summary of Servers Pane**

**Summary of Servers**

**Configuration** Control

A server is an instance of WebLogic Server that runs in its own Java Virtual Machine (JVM) and has its own configuration.  
This page summarizes each server that has been configured in the current WebLogic Server domain.

[Customize this table](#)

**Servers (Filtered - More Columns Exist)**

New Clone Delete Showing 1 to 4 of 4 Previous | Next

| <input type="checkbox"/> | Name               | Cluster | Machine      | State    | Health | Listen Port |
|--------------------------|--------------------|---------|--------------|----------|--------|-------------|
| <input type="checkbox"/> | AdminServer(admin) |         |              | RUNNING  | OK     | 7001        |
| <input type="checkbox"/> | WLS_Custom         |         | LocalMachine | SHUTDOWN |        | 8887        |
| <input type="checkbox"/> | WLS_Portlet        |         | LocalMachine | RUNNING  | OK     | 8889        |
| <input type="checkbox"/> | WLS_Spaces         |         | LocalMachine | RUNNING  | OK     | 8888        |

New Clone Delete Showing 1 to 4 of 4 Previous | Next

- Click the Portlet server (for example, `WLS_Portlet`) to configure the identity and trust keystores.  
The Settings pane for the Portlet server displays (see [Figure 14-47](#)).

**Figure 14–47 Settings Pane for Portlet Server**

**Settings for WLS\_Spaces**

Configuration Protocols Logging Debug Monitoring Control Deployments Services Security Notes

General Cluster Services Keystores SSL Federation Services Deployment Migration Tuning Overload

Health Monitoring Server Start

Save

Use this page to configure general features of this server such as default network communications.

[View JNDI Tree](#)

|  |                                    |  |
|--|------------------------------------|--|
| <b>Name:</b>   | WLS_Spaces                         | An alphanumeric name for this server instance. <a href="#">More Info...</a>  |
| <b>Machine:</b>  | LocalMachine                       | The WebLogic Server host computer (machine) on which this server is meant to run. <a href="#">More Info...</a>                   |
| <b>Cluster:</b>  | (Stand-Alone)                      | The cluster, or group of WebLogic Server instances, to which this server belongs. <a href="#">More Info...</a>                   |
| <b>Listen Address:</b>   | <input type="text"/>               | The IP address or DNS name this server uses to listen for incoming connections. <a href="#">More Info...</a>                     |
| <input checked="" type="checkbox"/> <b>Listen Port Enabled</b> |                                    | Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. <a href="#">More Info...</a>  |
| <b>Listen Port:</b>  | <input type="text" value="8888"/>  | The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. <a href="#">More Info...</a>    |
| <input type="checkbox"/> <b>SSL Listen Port Enabled</b>        |                                    | Indicates whether the server can be reached through the default SSL listen port. <a href="#">More Info...</a>                    |
| <b>SSL Listen Port:</b>  | <input type="text" value="8788"/>  | The TCP/IP port at which this server listens for SSL connection requests. <a href="#">More Info...</a>                           |
| <input type="checkbox"/> <b>Client Cert Proxy Enabled</b>      |                                    | Specifies whether the HttpClusterServlet proxies the client certificate in a special header. <a href="#">More Info...</a>        |
| <b>Java Compiler:</b>  | <input type="text" value="javac"/> | The Java compiler to use for all applications hosted on this server that need to compile Java code. <a href="#">More Info...</a> |

4. Open the **Configuration** tab, and then the **Keystores** subtab.  
The Keystores pane displays (see [Figure 14–48](#)).

Figure 14–48 Keystores Pane

Settings for WLS\_Spaces

Configuration Protocols Logging Debug Monitoring Control Deployments Services Security Notes

General Cluster Services **Keystores** SSL Federation Services Deployment Migration Tuning Overload

Health Monitoring Server Start

Save

Keystores ensure the secure storage and management of private keys and trusted certificate authorities (CAs). This page lets you view and define various keystore configurations. These settings help you to manage the security of message transmissions.

**Keystores:** Custom Identity and Java Standard Trust  Which configuration rules should be used for finding the server's identity and trust keystores? [More Info...](#)

**Identity**

**Custom Identity Keystore:**  The path and file name of the identity keystore. [More Info...](#)

**Custom Identity Keystore Type:**  The type of the keystore. Generally, this is JKS. [More Info...](#)

**Custom Identity Keystore Passphrase:**  The encrypted custom identity keystore's passphrase. If empty or null, then the keystore will be opened without a passphrase. [More Info...](#)

**Confirm Custom Identity Keystore Passphrase:**

**Trust**

**Java Standard Trust Keystore:** /u01/app/oracle/product/IR11/fmwhome/jdk160\_05\_R27.6.1-25/jre/lib/security/cacerts The path and file name of the trust keystore. [More Info...](#)

**Java Standard Trust Keystore Type:** jks The type of the keystore. Generally, this is JKS. [More Info...](#)

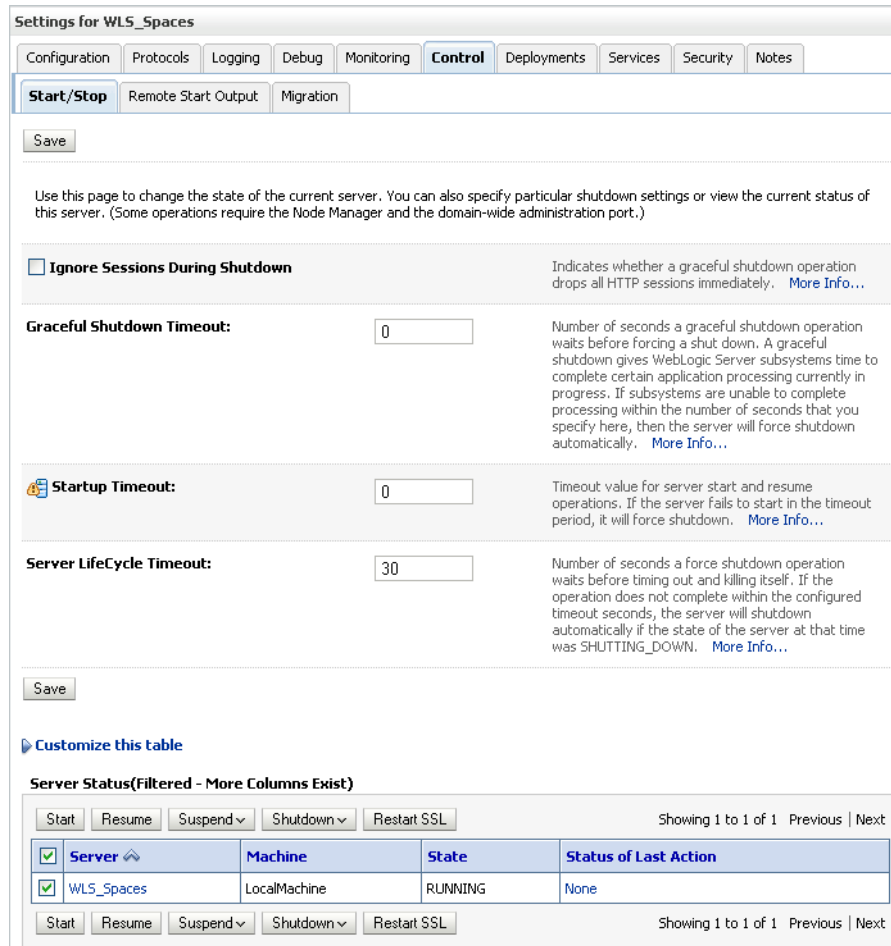
**Java Standard Trust Keystore Passphrase:**  The password for the Java Standard Trust keystore. This password is defined when the keystore is created. [More Info...](#)

**Confirm Java Standard Trust Keystore Passphrase:**

Save

5. For Keystores, select **Custom Identity and Java Standard Trust** and click **Save**.
6. Open the Control tab.  
The Control Settings pane displays (see [Figure 14–49](#)).

**Figure 14–49 Control Settings Pane**



7. Click **Restart SSL**.

**Configure the SSL connection**

1. In the Domain Structure pane, expand **Environment** and select **Servers**.
2. Click on the Portlet server (for example, *WLS\_Portlet*) for which you want to configure SSL.
3. Select **Configuration**.
4. Check **SSL Listen Port Enable**.
5. Enter a listen port number.
6. Select **Configuration > SSL**, and then open the Advanced options at the bottom of the page.
7. Select the **Two Way Client Cert Behavior** attribute and choose the **Client Certs Not Requested** option.
8. Click **Save**.
9. Restart the WebLogic Server and open the SSL URL.
10. Accept the certificate for the session and log in.

**Register the SSL-enabled WSRP producer and run the portlets**

1. Configure the WebCenter Spaces managed server to use the Custom Identity and Java Standard Trust store. This also uses the certificates in `javahome/jre/lib/security/cacerts`.
2. Download the certificate of the HTTPS producer URL and save it in `.PEM` format.  
Use Firefox 3.0 or later to download the certificate directly to `.PEM` format, or for other browsers use the WLS `der2pem` tool to convert to PEM format. For more information about using the `der2pem` tool, see "der2pem" in the *Oracle Fusion Middleware Command Reference for Oracle WebLogic Server*. Note that WebLogic does not recognize any other format other than `.PEM` format.
3. Import the certificate into the `cacerts` file in `JAVAHOME/jre/lib/security` using the following `keytool` command:

```
keytool -importcert -alias portlet_cert -file HOME/portlet_pem -keystore
./cacerts -storepass password
```

Where:

- `portlet_cert` is the portlet certificate alias
  - `portlet_pem` is the portlet certificate file (for example, `portlet_cert.pem`)
  - `password` is the keystore password
4. Restart `WLS_Spaces`.
  5. Start WLST as described in [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands"](#)
  6. Connect to the Administration Server for the target domain with the following command:

```
connect('user_name', 'password', 'host_id:port')
```

Where:

- `user_name` is the name of the user account with which to access the `WLS_Spaces` server (for example, `weblogic`)
  - `password` is the password with which to access the `WLS_Spaces` server
  - `host_id` is the host ID of the Administration Server
  - `port` is the port number of the Administration Server (for example, `7001`).
7. Run the `registerWSRPProducer` WLST command to register the producer:

```
registerWSRPProducer('webcenter', 'sslwsrpprod', 'producer_wsd1')
```

Where:

- `sslwsrpprod` is the name of the SSL-enabled WSRP producer
- `producer_wsd1` is the WSDL URL of the SSL-enabled WSRP producer

For example:

```
registerWSRPProducer('webcenter',
'sslwsrpprod', 'https://example.oracle.com:7004/richtextportlet/portlets/wsrp2?W
SDL')
```

8. Navigate to the HTTP or HTTPS WebCenter URL.

9. Create a page and go to the Portlets link.
10. Go to the registered WSRP producer.
11. Add the portlet to the page.
12. Go to the view mode of the page and check that the WSRP portlet renders correctly.

**Register the SSL-enabled PDK-Java Producer and run the portlets**

1. Configure the WebCenter Spaces managed server to use the Demo Identity and Trust store. This also uses the certificates in `javahome/jre/lib/security/cacerts`.

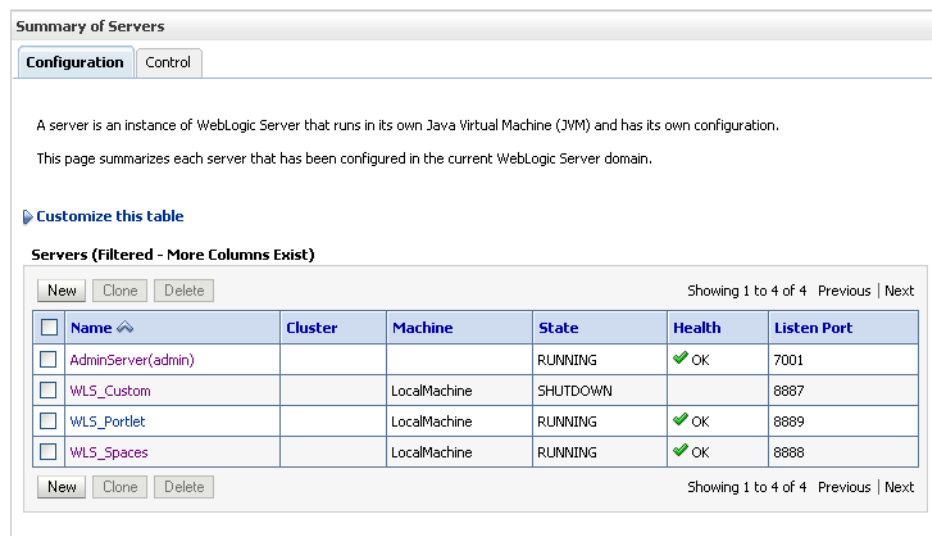
2. Log in to the WLS Administration Console.

For information on logging into the WLS Administration Console, see [Section 1.12.2, "Oracle WebLogic Server Administration Console"](#).

3. On the Domain Structure pane, expand **Environment** and click **Servers**.

The Summary of Servers pane displays (see [Figure 14–50](#)).

**Figure 14–50 Summary of Servers Pane**



4. Click `WLS_Spaces` in the servers list.

The Settings pane displays (see [Figure 14–51](#)).

**Figure 14–51 Settings Pane (WLS\_Spaces Server)**

Settings for WLS\_Spaces

Configuration Protocols Logging Debug Monitoring Control Deployments Services Security Notes

General Cluster Services Keystores SSL Federation Services Deployment Migration Tuning Overload

Health Monitoring Server Start

Save

Use this page to configure general features of this server such as default network communications.

[View JNDI Tree](#)

|  |                                    |  |
|--|------------------------------------|--|
| <b>Name:</b>   | WLS_Spaces                         | An alphanumeric name for this server instance. <a href="#">More Info...</a>  |
| <b>Machine:</b>  | LocalMachine                       | The WebLogic Server host computer (machine) on which this server is meant to run. <a href="#">More Info...</a>                   |
| <b>Cluster:</b>  | (Stand-Alone)                      | The cluster, or group of WebLogic Server instances, to which this server belongs. <a href="#">More Info...</a>                   |
| <b>Listen Address:</b>   | <input type="text"/>               | The IP address or DNS name this server uses to listen for incoming connections. <a href="#">More Info...</a>                     |
| <input checked="" type="checkbox"/> <b>Listen Port Enabled</b> |                                    | Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. <a href="#">More Info...</a>  |
| <b>Listen Port:</b>  | <input type="text" value="8888"/>  | The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. <a href="#">More Info...</a>    |
| <input type="checkbox"/> <b>SSL Listen Port Enabled</b>        |                                    | Indicates whether the server can be reached through the default SSL listen port. <a href="#">More Info...</a>                    |
| <b>SSL Listen Port:</b>  | <input type="text" value="8788"/>  | The TCP/IP port at which this server listens for SSL connection requests. <a href="#">More Info...</a>                           |
| <input type="checkbox"/> <b>Client Cert Proxy Enabled</b>      |                                    | Specifies whether the HttpClusterServlet proxies the client certificate in a special header. <a href="#">More Info...</a>        |
| <b>Java Compiler:</b>  | <input type="text" value="javac"/> | The Java compiler to use for all applications hosted on this server that need to compile Java code. <a href="#">More Info...</a> |

Advanced

Save

5. Open the Configuration tab and select the Keystores tab.
6. Make sure that the value for **Demo Identity and Demo Trust** is either `jks` or left blank.
7. Click **Save**.
8. Download the certificate of the HTTPS producer URL and save it in `.PEM` format.  
Use Firefox 3.0 or later to download the certificate directly to `.PEM` format, or for other browsers use the `WLS der2pem` tool to convert to PEM format. For more information about using the `der2pem` tool, see "der2pem" in the *Oracle Fusion Middleware Command Reference for Oracle WebLogic Server*. Note that WebLogic does not recognize any other format other than `.PEM` format.
9. Import the certificate into the `cacerts` file in `JAVAHOME/jre/lib/security` using the following keytool command:

```
keytool -importcert HOME/portlet_cert.pem -keystore ./cacerts -storepass changeit
```
10. Restart WLS\_Spaces.
11. Start WLST as described in [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands"](#).

12. Connect to the Administration Server for the target domain with the following command:

```
connect('user_name','password','host_id:port')
```

where:

- *user\_name* is the name of the user account with which to access the WLS\_Spaces server (for example, weblogic)
- *password* is the password with which to access the WLS\_Spaces server
- *host\_id* is the host ID of the Administration Server
- *port* is the port number of the Administration Server (for example, 7001).

13. Run the `registerPDKJavaProducer` command:

```
registerPDKJavaProducer('webcenter','ssljpdkprod','producer_wsd1')
```

Where:

- *ssljpdkprod* is the name of the SSL-enabled PDK-Java producer
- *producer\_wsd1* is the WSDL URL of the SSL-enabled PDK-Java producer

This will enable one-way SSL for a Web producer. That is, only the server side (web producer) uses certificates. The Web producer code also uses a shared key feature (discussed later) for client authentication.

14. Go to the HTTP or HTTPS WebCenter URL.
15. Create a page and go to the Portlets link.
16. Go to the registered PDK-Java producer.
17. Add the portlet to the page.
18. Go to the view mode of the page and check that the PDK-Java portlet renders correctly.

### 14.6.6 Securing the WebCenter Spaces Connection to the LDAP Identity Store

To configure the LDAP server port for SSL, refer to the appropriate administration documentation for the LDAP server. For Oracle Internet Directory (OID), an SSL port is installed by default. To use this port for LDAP communication from WebCenter, the identity store should be configured for authentication with the appropriate authenticator. See [Section 14.3, "Configuring the Identity Store"](#) for the steps to do this for the identity store.

---

---

**Note:** When entering the Provider Specific information, be sure to specify an SSL port and to check the SSL Enabled checkbox.

---

---

If the CA is unknown to the Oracle WebLogic server, complete the two additional steps described in the following subsections:

- [Exporting the OID Certificate Authority \(CA\)](#)
- [Setting Up the WebLogic Server](#)

For more information, see "Setting Up a One- Way SSL Connection" in the *Oracle Fusion Middleware Security Guide*.



### 14.6.6.1 Exporting the OID Certificate Authority (CA)

If the CA is unknown to the Oracle WebLogic server (the command prompts the user to enter the keystore password) you will need to use `orapki` to create a certificate. The following example shows how to use this command to create the certificate `serverTrust.cert`:

```
orapki wallet export -wallet CA -dn "CN=myCA" -cert oid_server_trust.cert
```

### 14.6.6.2 Setting Up the WebLogic Server

If the CA is unknown to the Oracle WebLogic server, use the utility `keytool` to import the Oracle Internet Directory's CA into the WebLogic trust store. The following example shows how to use `keytool` to import the file `oid_server_trust.cert` into the server trust store `cacerts`:

```
keytool -importcert -v -trustcacerts -alias oid_server_trust -file oid_server_trust.cer -keystore cacerts -storepass changeit
```

## 14.6.7 Securing the WebCenter Spaces Connection to OCS with SSL

For instructions on how to configure Oracle Content Server (OCS) for SSL, see [Section 10.2.1.2.3, "Configuring Secure Socket Layer \(SSL\)"](#). For instructions on adding a trusted certificate to the WebCenter Spaces trust store, see the section on importing the certificate into the trust store in [Section 14.6.1.2, "Configuring the Identity and Trust Keystores"](#).

## 14.6.8 Securing the WebCenter Spaces Connection to IMAP and SMTP with SSL

Before associating you need to first import the certificate into the trust store. Follow the steps below to put the certificate in the trust store and configure WebCenter Spaces to use the trust store.

To secure the WebCenter Spaces connection to IMAP and SMTP with SSL:

1. Open a browser and connect to your IMAP server with the following command:

```
https://imapserver:ssl_port
```

For example:

```
https:mailserver.example:993
```

2. Place your cursor on the page, right-click, and select **Properties**.
3. Click **Certificate**.
4. In the popup window, click the **Details** tab and click **Copy to File...**

Be sure to use the DER encoded binary (X.509) format and copy to a file.

5. Convert the .DER format certificate to .PEM format.

Use Firefox 3.0 or later to download the certificate directly to .PEM format, or for other browsers use the WLS `der2pem` tool to convert to PEM format. For more information about using the `der2pem` tool, see "der2pem" in the *Oracle Fusion Middleware Command Reference for Oracle WebLogic Server*. Note that WebLogic does not recognize any other format other than .PEM format.

6. Import the certificate into the `cacerts` in the `jdk_home` using the following command:

```
keytool -import -alias imap_cer -file cert_file.cer -keystore cacerts -storepass changeit
```

Where *cert\_file* is the name of the certificate file you downloaded.

7. Register the mail server connection as described in [Section 11.3.3, "Registering Mail Servers"](#).
8. Restart Webcenter Spaces.
9. Log into WebCenter Spaces and provide your mail credentials.

### 14.6.9 Securing the WebCenter Spaces Connection to Oracle SES with SSL

Before associating you need to first import the certificate into the trust store. Follow the steps below to put the certificate in the trust store and register the Oracle Secure Enterprise Search (SES) connection.

To download the certificate of the HTTPS URL and save it:

1. Use your browser to navigate to the Web Services URL that Oracle Secure Enterprise Search exposes to enable search requests at:

```
http://host:port/search/query/OracleSearch
```

For example:

```
https://example.com:7777/search/query/OracleSearch
```

2. Place your cursor on the page, right-click with your mouse, and select **Properties**.
3. Click **Certificate**.

4. In the popup window, open the Details tab, and click **Copy to File...**

Use **DER encoded binary(X.509)** format and copy the certificate to a file.

5. Convert the .DER format certificate to .PEM format.

Use Firefox 3.0 or later to download the certificate directly to .PEM format, or for other browsers use the WLS `der2pem` tool to convert to PEM format. For more information about using the `der2pem` tool, see "der2pem" in the *Oracle Fusion Middleware Command Reference for Oracle WebLogic Server*. Note that WebLogic does not recognize any other format other than .PEM format.

6. Import the certificate into `DemoTrustKeyStore.jks` or `cacerts` in the `jdk_home` using one of the following commands:

```
keytool -import -alias ses_cer -file cert_file.cer -keystore cacerts -storepass changeit
```

where *cert\_file* is the name of the certificate file you downloaded.

7. Register the SES connection as described in [Section 11.4.3, "Registering Oracle Secure Enterprise Search Services"](#).
8. Restart WebCenter Spaces.

### 14.6.10 Securing the WebCenter Spaces Connection to OWLCS with SSL

To secure the WebCenter Spaces connection to Oracle WebLogic Communication Services (OWLCS) with SSL, follow the steps below to import the certificate into the truststore, and point WebCenter Spaces to use the truststore. Note that securing the WebCenter Spaces connection to OWLCS with SSL is optional since OWLCS can be configured with confidentiality using WS-Security. See [Section 14.8.3, "Securing Oracle WebLogic Communication Services \(OWLCS\) with WS-Security"](#).

Before associating you need to first import the certificate into the truststore. Follow the steps below to put the certificate in the truststore:

1. Open your browser and go to the OWLCS server (for example, `https://example.com:port/PresenceConsumerService/services/PresenceConsumer`)
2. Place your cursor on the page, right-click, and select **Properties**.
3. Click **Certificate**.
4. In the popup window, open the **Details** tab and click **Copy to File...**  
Use Firefox 3.0 or later to download the certificate directly to .PEM format, or for other browsers use the WLS `der2pem` tool to convert to PEM format. For more information about using the `der2pem` tool, see "der2pem" in the *Oracle Fusion Middleware Command Reference for Oracle WebLogic Server*. Note that WebLogic does not recognize any other format other than .PEM format.
5. Import the certificate into the `cacerts` using the following keytool command:  

```
keytool -import -alias owlcs_cer -file cert_file.cer -keystore cacerts -storepass changeit
```

  
where `cert_file` is the name of the certificate file you downloaded.
6. Locate the `cacerts` file used by the OWLCS server in the OWLCS installation, and also update the OWLCS referenced `cacerts` file with this certificate:  

```
keytool -import -alias owlcs_cer -file cert_file.cer -keystore cacerts -storepass changeit
```
7. Register the Oracle WebLogic Communication Services connection as described in [Section 11.2.3, "Registering Instant Messaging and Presence Servers"](#).
8. Restart the WebCenter Spaces server.

### 14.6.11 Securing the WebCenter Spaces Connection to Microsoft Live Communication Server with SSL

To secure the WebCenter Spaces connection to Microsoft Live Communication Server with SSL, follow the steps below to import the certificate into the truststore, and point WebCenter Spaces to use the truststore. Note that securing the WebCenter Spaces connection to Microsoft Live Communication Server with SSL is optional since Microsoft Live Communication Server can be configured with confidentiality using WS-Security.

Before associating you need to first import the certificate into the truststore. Follow the steps below to put the certificate in the truststore:

1. Open your browser and go to the Microsoft Live Communication Server (for example, `https://example.com:port/PresenceConsumerService/services/PresenceConsumer`)
2. Place your cursor on the page, right-click, and select **Properties**.
3. Click **Certificate**.
4. In the popup window, open the **Details** tab and click **Copy to File...**  
Use Firefox 3.0 or later to download the certificate directly to .PEM format, or for other browsers use the WLS `der2pem` tool to convert to PEM format. For more

information about using the `der2pem` tool, see "der2pem" in the *Oracle Fusion Middleware Command Reference for Oracle WebLogic Server*. Note that WebLogic does not recognize any other format other than .PEM format.

5. Import the certificate into the `cacerts` using the following `keytool` command:

```
keytool -import -alias lcs_cer -file cert_file.cer -keystore cacerts -storepass changeit
```

where `cert_file` is the name of the certificate file you downloaded.

6. Locate the `cacerts` file used by the Microsoft Live Communication Server in the Microsoft Live Communication Server installation, and also update the Microsoft Live Communication Server referenced `cacerts` file with this certificate:

```
keytool -import -alias lcs_cer -file cert_file.cer -keystore cacerts -storepass changeit
```

7. Register the Microsoft Live Communication Server connection as described in [Section 11.2.3, "Registering Instant Messaging and Presence Servers"](#).
8. Restart the WebCenter Spaces server.

## 14.7 Configuring a WebCenter Application to Use Single Sign-On

Oracle Access Manager (OAM), part of Oracle's enterprise class suite of products for identity management and security, provides a wide range of identity administration and security functions, including several single sign-on options for WebCenter Spaces and custom WebCenter applications. OAM is the recommended single sign-on solution for Oracle WebCenter 11g installations.

For deployment environments that are already invested in Oracle 10g infrastructure, and where the Oracle Application Server Single Sign-On (OSSO) server is used as the primary SSO solution, WebCenter 11g can also be configured to use OSSO for single sign-on.

For smaller scale Oracle WebCenter 11g installations, where you do not have an enterprise-class single sign-on infrastructure like Oracle Access Manager or Oracle SSO, and you only need to provide a single sign-on capability within WebCenter Spaces and its associated web applications like Wiki, Discussions, RSS and Worklist, you can configure a SAML-based SSO solution. If you need to provide single sign-on with other enterprise applications, this solution is not recommended.

If your enterprise uses Microsoft desktop logins that authenticate with a Microsoft domain controller with user accounts in Active Directory, then configuring SSO with Microsoft Clients may also be an option to consider.

The setup required for each of these SSO solutions is described in the following subsections:

- [Section 14.7.1, "Configuring Oracle Access Manager \(OAM\)"](#)
- [Section 14.7.2, "Configuring Oracle Single Sign-On \(OSSO\)"](#)
- [Section 14.7.3, "Configuring SAML-based Single Sign-on"](#)
- [Section 14.7.4, "Configuring SSO with Microsoft Clients"](#)

### 14.7.1 Configuring Oracle Access Manager (OAM)

Oracle Access Manager (OAM) provides flexible and extensible authentication and authorization, and provides audit services. This section describes how to configure

WebCenter Spaces and custom WebCenter applications for OAM single sign-on authentication, including how to configure the WebLogic server side and the WebCenter application as the partner application participating in SSO.

Much of the configuration can be done using scripts (recommended). To use the scripts, follow the instructions in [Section 14.7.1.2, "Configuring OAM Using Scripts,"](#) and complete the instructions in [Section 14.7.1.3, "Configuring the Webtier Components"](#) and [Section 14.7.1.6, "Configuring the Policy Manager,"](#) and any additional configurations as appropriate in [Section 14.7.1.7, "Additional Configurations."](#)

To perform the configuration manually, complete the instructions in all of the subsections, with the exception of [Section 14.7.1.2, "Configuring OAM Using Scripts."](#)

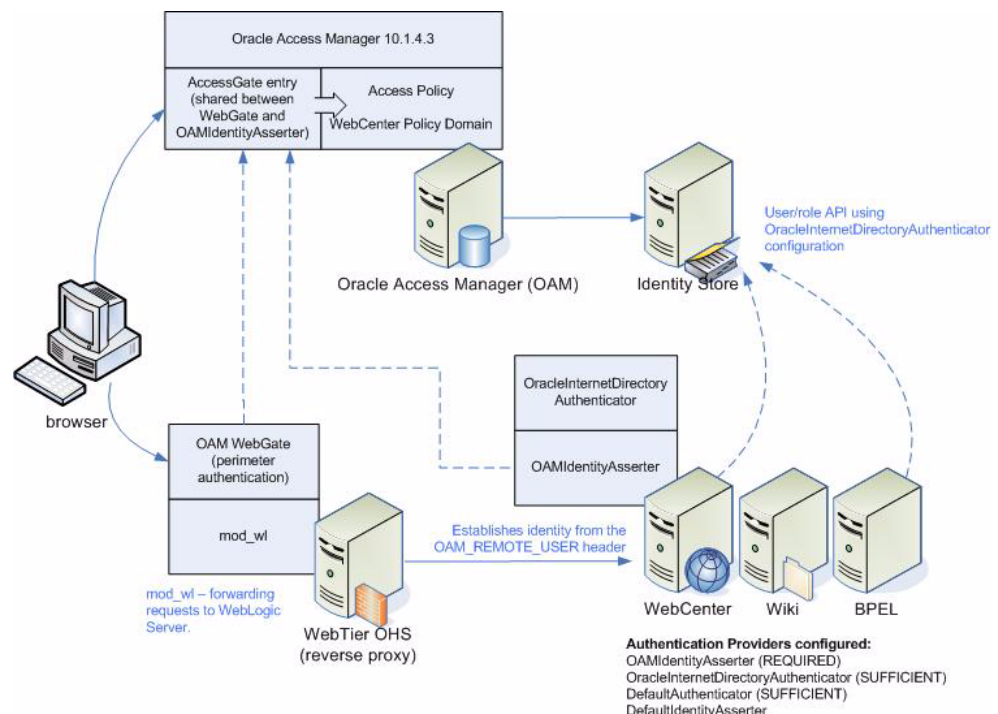
The scripted and equivalent manual configuration steps are presented in the following subsections:

- [OAM Components and Topology](#)
- [Configuring OAM Using Scripts](#)
- [Configuring the Webtier Components](#)
- [Manually Configuring the Access System](#)
- [Manually Defining the WebCenter Policy Domain](#)
- [Configuring the Policy Manager](#)
- [Additional Configurations](#)

### 14.7.1.1 OAM Components and Topology

[Figure 14–52](#) shows the components and topology required to set up single sign-on with Oracle Access Manager for a WebCenter application.

**Figure 14–52 OAM Single Sign-On Components and Topology**



OAM consists of the following components:

- **Access Server** - a standalone server that provides authentication, authorization, and auditing services for Access Gates. There is one access server set up on OAM. This is done as part of the OAM install itself.
- **WebGate** - an out-of-the-box plugin that intercepts Web resource (HTTP) requests and forwards them to the Access Server for authentication and authorization.
- **Identity Assertion Provider (IAP)** - a type of security provider that asserts the identity of the user based on header information that is set by perimeter authentication. The OAM integration provides an OAM ID Asserter that can be configured as the OAM IAP. The OAM ID Asserter can be used for authentication or for identity assertion. For OAM SSO integration, the OAM ID Asserter should be configured as an Identity Assertion Provider (IAP) by selecting `obSSOCookie` under **Active Types** in the provider's Common settings.

### 14.7.1.2 Configuring OAM Using Scripts

These steps assume that you've installed Oracle WebCenter (see [Section 2.3, "Installing WebCenter Spaces"](#)). By default, an Oracle WebCenter installation creates a WLS domain, including an Administration Server and three managed servers: `WLS_Spaces`, `WLS_Services` and `WLS_Portlet`.

1. Install the WebTier, which contains the Oracle HTTP Server (OHS) and `mod_wl` (see the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter* for information on how to install the WebTier).
2. Configure the module `mod_wl` in the WebTier OHS so that it forwards requests to the Oracle WebLogic Server for WebCenter, as described in [Section 14.7.1.3.1, "Configure `mod\_weblogic` \(`mod\_wl\_ohs.conf`\)"](#).
3. Determine which access server to use.
  - a. Log onto the Access Manager.
  - b. Click **Access System Console**.
  - c. Open the Access System Configuration tab.
  - d. Click **Access Server Configuration** to display a list of all access servers.
  - e. Click an access server in the list to see server details.

The host name and port are the values you need for the `oam_aaa_host` and `oam_aaa_port` parameters respectively in the script.

4. Run the following command.

The `oamcfgtool.jar` is available in `ORACLE_HOME/modules/oracle.oamprovider_11.1.1/oamcfgtool.jar` in the WebCenter installation. Values in bold are the one that you need to supply based on the settings of your WebCenter and OAM instances.

```
java -jar $ORACLE_HOME/modules/oracle.oamprovider_11.1.1/oamcfgtool.jar
mode=CREATE app_domain="your_domain_name"
protected_uris="/webcenter/adfAuthentication,/owc_wiki/user/login.jsp,/owc_
wiki/adfAuthentication,/integration/worklistapp,
/workflow/sdpmessaging-sca-ui-worklist/faces/adf.task-flow,/workflow/WebCenterWo
rklistDetail/faces/adf.task-flow,
/workflow/sdpmessaging-sca-ui-worklist,/rss/rsservlet,/owc_
discussions/login!withRedirect.jspa,
/owc_discussions/login!default.jspa,/owc_discussions/login.jspa,/owc_
discussions/admin"
```

```
public_uris="/webcenter,/owc_wiki,/owc_discussions,/rss,/workflow"
app_agent_password=<Password to be provisioned for App Agent>
ldap_host=<Hostname of LDAP server> ldap_port=<Port of LDAP server>
ldap_userdn=<DN of LDAP Admin User, usually "cn=orcladmin">
ldap_userpassword=<Password of LDAP Admin User> oam_aaa_host=<HOST of OAM
server> oam_aaa_port=<Port of OAM server>
```

We recommend that you register your domain (for <your\_domain\_name>) as something like "webtier.example.com", where "webtier.example.com" is your Webtier, so that you can easily distinguish the various policies in OAM.

If your command ran successfully, you should see something like the following output depending on the values you used:

```
Processed input parameters
Initialized Global Configuration
Successfully completed the Create operation.
Operation Summary:
Policy Domain : webtier.example.com
Host Identifier: webtier.example.com
Access Gate ID : webtier.example.com_AG
```

You can also run the Validate command to validate your configurations:

```
java -jar ORACLE_HOME/modules/oracle.oamprovider_11.1.1/oamcfgtool.jar
mode=VALIDATE app_domain="your_domain_name"
ldap_host=<Hostname of LDAP server> ldap_port=<Port of LDAP server>
*ldap_userdn=<DN of LDAP Admin User, usually "cn=orcladmin"*
ldap_userpassword=<Password of LDAP Admin User> oam_aaa_host=<HOST of OAM
server> oam_aaa_port=<Port of OAM server>
test_username=<Username to be used for policy validation> test_
userpassword=<Userpassword to be used for policy validation>
```

If your command runs successfully, you should see the same output as above.

## 5. Check the Policy Domain settings.

- a. Log on to the Oracle Access Manager.
- b. Click **Policy Manager**.
- c. Click **My Policy Domains**.

You should see the domain you just created in the list of policy domains. In the URL prefixes column, you should also see the URIs you specified during the creation of this domain.

- d. Click the domain you just created and open the Resources tab.

The URIs you specified should be showing. You can also open other tabs to view and verify other settings, and manually add additional resources later, if required.

## 6. Check the Access Gate Configurations.

- a. Click on **Access System Console**.
- b. Open the Access System Configuration tab.
- c. Click **AccessGate Configuration**.
- d. Enter some search criteria and click **Go**.
- e. When the Access Gate for the domain you just created shows up (it will have the suffix `_AG`), click on it to see the setting details.



7. Run the WebGate Installer as described in the section on "Installing the WebGate" in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*.

The InstallShield Wizard will prompt you for several inputs during the installation. Supply the information requested based on the settings for your environment.

8. Continue with the steps for configuring the Policy Manager in [Section 14.7.1.6, "Configuring the Policy Manager"](#), and any further configurations, as required, in [Section 14.7.1.7, "Additional Configurations"](#).

### 14.7.1.3 Configuring the Webtier Components

Configuring the Webtier components is described in the following sections:

- [Configure mod\\_weblogic \(mod\\_wl\\_ohs.conf\)](#)
- [Create an AccessGate Entry](#)
- [Install WebGate on the WebTier](#)

#### 14.7.1.3.1 Configure mod\_weblogic (mod\_wl\_ohs.conf)

Configure the module `mod_wl` in the WebTier OHS so that it forwards requests to the Oracle WebLogic Server for WebCenter, by uncommenting lines at `WEBTIER_HOME/instances/<your_instance>/config/OHS/ohs1/mod_wl_ohs.conf`. This file is included by the `httpd.conf` file.

To configure Web Tier OHS to work with multiple non-clustered servers, use the example below in `mod_wl_ohs.conf`. Make sure that the WebLogic port numbers match your configuration.

```
<IfModule mod_weblogic.c>
MatchExpression /webcenter WebLogicHost=webcenter.example.com|WebLogicPort=8888
MatchExpression /rss WebLogicHost=webcenter.example.com|WebLogicPort=8890
MatchExpression /owc_wiki WebLogicHost=webcenter.example.com|WebLogicPort=8890
MatchExpression /owc_discussions
WebLogicHost=webcenter.example.com|WebLogicPort=8890
MatchExpression /workflow WebLogicHost=soa.example.com|WebLogicPort=8888
MatchExpression /integration/worklistapp
WebLogicHost=soa.example.com|WebLogicPort=8888
MatchExpression /integration/services
WebLogicHost=soa.example.com|WebLogicPort=8888
MatchExpression /soa-infra WebLogicHost=soa.example.com|WebLogicPort=8888
</IfModule>
```

---

**Note:** The entries in the `MatchExpression` list above map the incoming paths to the appropriate WLS managed servers on which the corresponding applications reside.

---

#### 14.7.1.3.2 Create an AccessGate Entry

An `AccessGate` entry needs to be created on the Access Manager to be shared by the OAM Identity Assertion Provider (IAP), and the WebGate performing perimeter authentication on the webtier reverse proxy.



---

**Note:** If you are doing the configuration using the `oamcfgtool` scripted installation, this step is not required, as the installation script does it automatically.

---

To create an AccessGate entry:

1. Log in to the Access Server Console using your browser to navigate to:

`http://host:port/access/oblix`

Where *host* is the host ID of the server hosting the Access Manager (for example, `oam.example.com`), and *port* is the HTTP port number (for example, 8888).

2. Open the Access System Configuration page.
3. Click **Add New AccessGate** to create a new AccessGate entry.
4. Click **List Access Servers** on the Details pane and bind the AccessGate to the Access Server that has been set up for OAM Single Sign-on.

Some of the settings specified here will be needed for WebGate installation and OAM Identity Assertion Provider (IAP) setup. [Table 14-2](#) shows settings for a typical AccessGate entry.

**Table 14-2 Sample Settings for AccessGate Entry**

| Setting                             | Value                 |
|-------------------------------------|-----------------------|
| AccessGate Name                     | webcenter-access-gate |
| Description                         |                       |
| State                               | Enabled               |
| Hostname                            | webtier.example.com   |
| Port                                | 9010                  |
| Access Gate Password                | <Not Displayed>       |
| Debug                               | Off                   |
| Maximum user session time (seconds) | 3600                  |
| Idle Session Time (seconds)         | 3600                  |
| Maximum Connections                 | 1                     |
| Transport Security                  | Open                  |
| IPValidation                        | On                    |
| IPValidationException               |                       |
| Maximum Client Session Time (hours) | 24                    |
| Failover threshold                  | 1                     |
| Access server timeout threshold     |                       |
| Sleep For (seconds)                 | 60                    |
| Maximum elements in cache           | 100000                |
| Cache timeout (seconds)             | 1800                  |

**Table 14–2 (Cont.) Sample Settings for AccessGate Entry**

| Setting                    | Value                    |
|----------------------------|--------------------------|
| Impersonation username     |                          |
| Impersonation password     | <Not Displayed>          |
| <b>ASDK Client</b>         |                          |
| Access Management Service  | On                       |
| <b>Web Server Client</b>   |                          |
| Primary HTTP Cookie Domain | .example.com             |
| Preferred HTTP Host        | webtier.example.com:9010 |
| Deny On Not Protected      | Off                      |
| CachePragmaHeader          | no-cache                 |
| CacheControlHeader         | no-cache                 |
| LogOutURLs                 |                          |

#### 14.7.1.3.3 Install WebGate on the WebTier

This section describes how to install the WebGate.

To install the WebGate:

1. Copy the ZIP file (`Oracle_Access_Manager10_1_4_3_0_linux_GCClib.zip`) containing the two `gcc` libraries required for the installation (`libgcc_s.so.1` and `libstdc++.so.5`) to a `/tmp` directory.
2. Run the installation as `root`. For example, from the `/tmp` directory run:
 

```
sudo -u root ./Oracle_Access_Manager10_1_4_3_0_linux_OHS11g_WebGate
```
3. Follow the installation runtime instructions, providing the installation directory, information of the AccessGate that you created earlier and the absolute path to the `httpd.conf` file of the web server. For example:

```
WEBTIER_HOME/instances/instance1/config/OHS/ohs1/httpd.conf
```

Information for the AccessGate can be found in the Access System Console. For more information, see [Section 14.7.1.3.2, "Create an AccessGate Entry"](#).

4. After the installation a new section is inserted in the `httpd.conf` file between the following entries:

```
*** BEGIN WEBGATE SPECIFIC ***
*** END Oblix NetPoint Specific ***
```

Check to see if the content is consistent with your environment.

#### 14.7.1.4 Manually Configuring the Access System

To configure the Access System, you need to add a host identifier:

1. Log in to the Access Server Console using your browser to navigate to:

```
http://host:port/access/oblix
```

Where *host* is the host ID of the server hosting the Access Manager (for example, `oam.example.com`), and *port* is the HTTP port number (for example, 8888).

2. Open the Access System Configuration page.
3. On the navigation pane, click **Host Identifiers**.
4. Add a host identifier for the webtier and enter the **Host Identifier name** (for example, `webtier`), a **Description**, and all **Hostname variations**. The hostname variations should include all the ways that a browser could issue a request to the webtier. For example, `webtier` and `webtier.example.com` if the webtier is using the default port; and additionally `webtier:8080` and `webtier.example.com:8080` if the webtier is not using the default port.

#### 14.7.1.5 Manually Defining the WebCenter Policy Domain

This section describes the steps to set up the WebCenter Policy Domain that will configure the WebCenter application for OAM SSO authentication.

To configure the WebCenter Policy Domain:

1. Log in to the Access Server Console using your browser to navigate to:

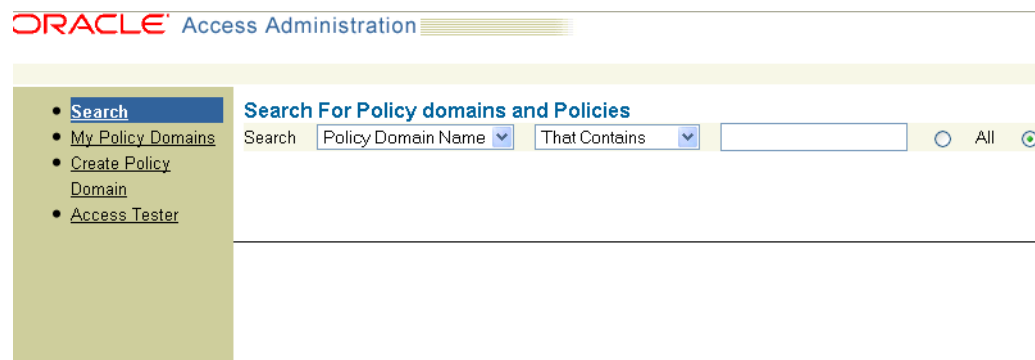
`http://host:port/access/oblix`

where *host* is the host ID of the server hosting the Access Manager (for example, `oam.example.com`), and *port* is the HTTP port number (for example, 8888).

2. Click **Policy Manager**.

The Policy Manager pane displays (see [Figure 14-53](#)).

**Figure 14-53 Policy Manager Pane**



3. Click **Create Policy Domain** in the Navigation pane to create a new policy domain to protect the WebCenter resources.

The Create Policy Domain page displays (see [Figure 14-54](#)).

**Figure 14–54 Create Policy Domain Page**

**Create Policy Domain**

General Resources Authorization Rules Default Rules Policies Delegated Access Admins

Name: webtier.example.com

Description: [Empty text area]

Save Cancel

4. Enter a Name (for example, `webtier.example.com`) and Description for the policy domain and click **Save**.
5. Open the Resources tab and click **Add**.  
The Resource page displays (see [Figure 14–55](#)).

**Figure 14–55 Policy Domain Resource Page**

webtier.example.com  
MyPolicyDomain > Resource

General Resources Authorization Rules Default Rules Policies Delegated Access Admins

Resource Type: http

Host Identifiers: webtier.example.com

URL Prefix: /owc\_wiki/user/login.jz

Description: [Empty text area]

Update Cache

Save Cancel

6. Add the resources that need to be secured. For each resource:
  - a. Select `http` as the **Resource Type**.
  - b. Select the **Host Identifier** for the WebCenter webtier.
  - c. Enter the **URL Prefix** for the resources you want to protect.

The following resources can be protected:

```

/adf.task-flow
/faces/adf.task-flow
/integration/worklistapp
/owc_discussions/login!withRedirect.jspa
/owc_discussions/login!default.jspa
/owc_discussions/login.jspa
/owc_discussions/admin
/owc_wiki/user/login.jz
/owc_wiki/acl
/owc_wiki/adfAuthentication
/owc_wiki/admin
    
```

```

/owc_wiki/attachments
/owc_wiki/default
/owc_wiki/domain
/owc_wiki/export
/owc_wiki/index_dir
/owc_wiki/install
/owc_wiki/js
/owc_wiki/layouts
/owc_wiki/macro
/owc_wiki/page
/owc_wiki/pages
/owc_wiki/remote
/owc_wiki/tags
/owc_wiki/templates
/owc_wiki/user
/owc_wiki/vhost
/owc_wiki/wp
/rss/rssservlet
/webcenter/adfAuthentication
/workflow/sdpmessagingsca-ui-worklist
/workflow/WebCenterWorklistDetail/faces
/workflow/sdpmessagingsca-ui-worklist

```

- d. Enter a **Description** for the resource.
  - e. Make sure that **Update Cache** is selected, and then click **Save**.
7. Open the Authorization Rules tab and click **Add**.
- The Authorization Rules page displays (see [Figure 14–56](#)).

**Figure 14–56 Authorization Rules Page**

The screenshot shows the 'Authorization Rules' configuration page. The 'Name' field contains 'Default\_Authorization' and the 'Description' field contains 'Default authorization rule for all URI accesses to app\_domain:webtier.example.com'. The 'Enabled' dropdown is set to 'Yes' and 'Allow takes precedence' is set to 'No'. The 'Update Cache' checkbox is checked. 'Save' and 'Cancel' buttons are at the bottom.

8. Enter a **Name** for the new rule (for example, Default\_Authorization) and **Description**.
  9. Select **Yes** for **Enabled**, and **No** for **Allow takes precedence**, and click **Save**.
  10. Click **Allow Access** on the Authorization Rules tab and click **Add**.
- The Allow Access page displays (see [Figure 14–57](#)).

**Figure 14–57 Allow Access Page**

11. In the **Role** drop down list, select **Any one** and click **Save**.

12. Open the **Default Rules** tab and click **Add**.

The Access Manager Authentication Rule page displays (see [Figure 14–58](#)).

**Figure 14–58 Access Manager Authentication Rules Page**

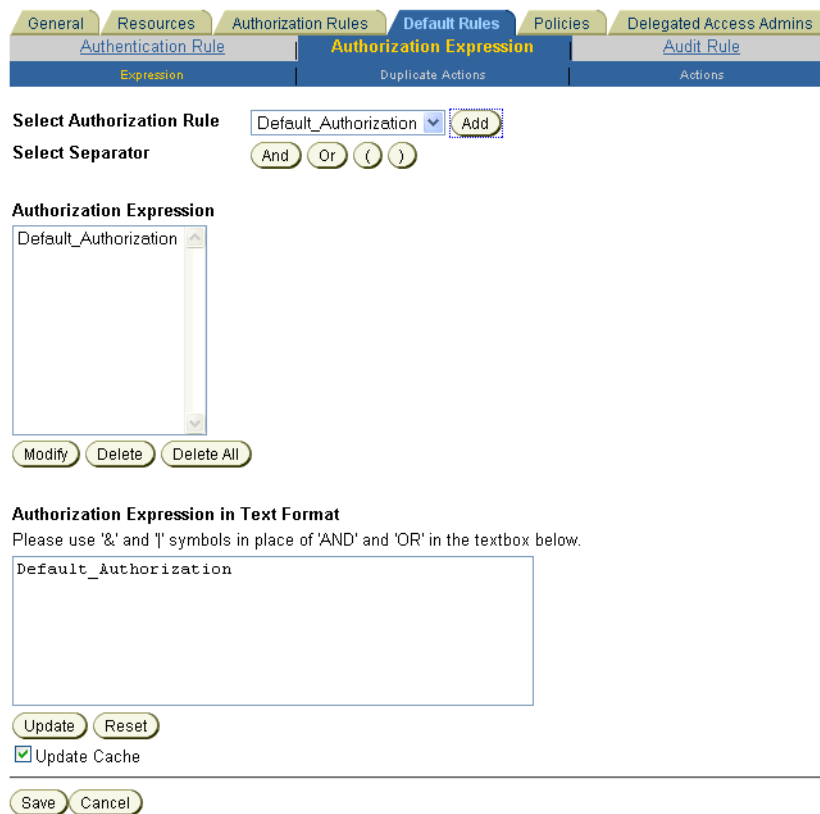
13. Enter a **Name** (for example, `Default_SSO`) and **Description** for the rule.

14. Set the **Authentication Scheme** to `Oracle: Form Authentication` (or a form-based authentication scheme that was previously created) and click **Save**.

15. Click **Authorization Expression** on the **Default Rules** tab, and click **Add**.

The Authorization Expression page displays (see [Figure 14–59](#)).

**Figure 14–59 Authorization Expression Page**

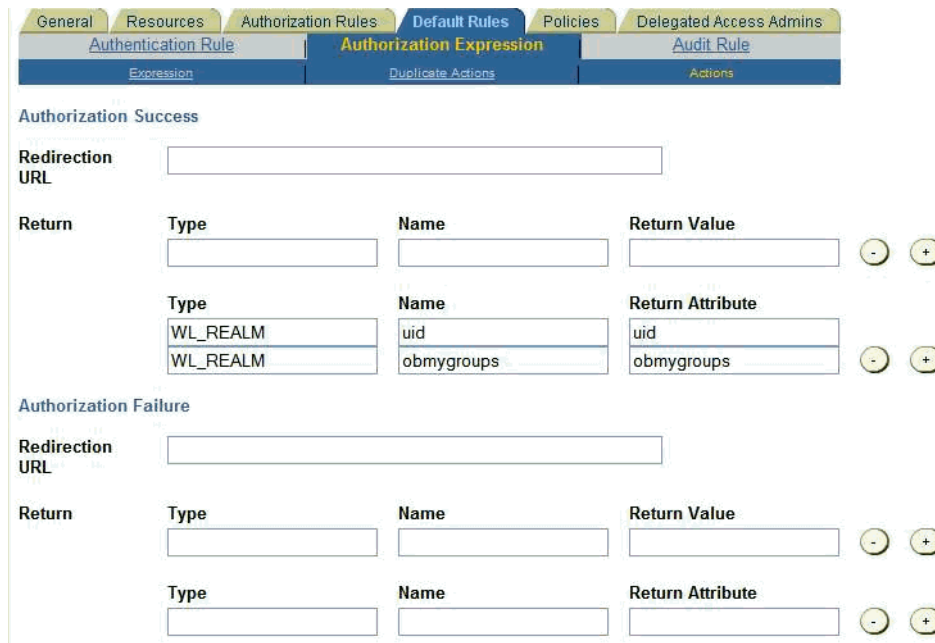


This screenshot shows the Access Manager's Authorization Expression page.

\*\*\*\*\*

16. Add the `Default-Authorization` authorization rule (or the rule you created previously) to the Authorization Expression and click **Add** to add it to the Authorization Expression list.
17. Click **Save**.
18. Click **Actions** on the Authorization Expression subtab and click **Add**.  
The Actions page displays (see [Figure 14–60](#)).

**Figure 14–60 Actions Page**



This screenshot shows the Access Manager's Actions page.

\*\*\*\*\*

19. Under Authorization Success, specify what actions should be invoked when the authorization succeeds. Add two **Return Attribute** entries, specifying the **Return Type**, **Name** and **Return Attribute** as:
  - HeaderVar, REMOTE\_USER, uid
  - HeaderVar, OAM\_REMOTE\_USER, uid

---

**Note:** Be careful not to put these values under the row for **Return Value**. The settings should be placed under **Return Attribute**.

---

20. Click **Save**.
21. Open the Policies tab and click **Add**.  
The Policies page displays (see [Figure 14–61](#)).



Figure 14–61 Policies Page

WebCenter Policy Domain > Policies

General Resources Authorization Rules Default Rules **Policies** Delegated Access Admins

**Name** WebCenter Protection Policy

**Description** Protected resources in WebCenter that should require authentication.

**Resource Type** http

**Resource Operation(s)**

GET  POST  PUT  
 HEAD  DELETE  TRACE  
 OPTIONS  CONNECT  OTHER

**Resource**

all

| Host Identifiers                    | URL Prefix                                  | Description   |
|-------------------------------------|---|---|
| <input type="checkbox"/> dadvma0006 | /owc_wiki                                   | Resource to protect and trigger authentication into the wiki app.     |
| <input type="checkbox"/> dadvma0006 | /workflow<br>/sdpmessagingsc<br>ui-worklist | Spaces task details app on the SOA server.                            |
| <input type="checkbox"/> dadvma0006 | /webcenter<br>/adfAuthentication            | WebCenter resource that triggers authentication to the WLS container. |

**URL Pattern**

22. Enter a **Name** (for example, Public URI Policy) and **Description** for the policy that will identify which resources are to be secured to trigger authentication.
23. Set the **Resource Type** to http.
24. Select GET, and POST as the **Resource Operations**.
25. Select the **Host Identifier** (the host identifier of the WebCenter webtier) to which to apply the policy (for example, webtier.example.com) and click **Save**.

#### 14.7.1.6 Configuring the Policy Manager

Configuring the Policy Manager is described in the subsections below.

- [Configuring the Oracle Internet Directory Authenticator](#)
- [Configuring the OAM Identity Asserter](#)
- [Configuring the Default Authenticator and Setting the Provider Order](#)
- [Configuring the Application for Oracle Access Manager SSO](#)

##### 14.7.1.6.1 Configuring the Oracle Internet Directory Authenticator

Assuming Oracle Internet Directory is backing the OAM identity store, an Oracle Internet Directory authenticator (`OracleInternetDirectoryAuthenticator`) should be configured for the LDAP server that is used as the identity store of OAM, and the provider should be set to `SUFFICIENT`.

To configure the Oracle Internet Directory authenticator:

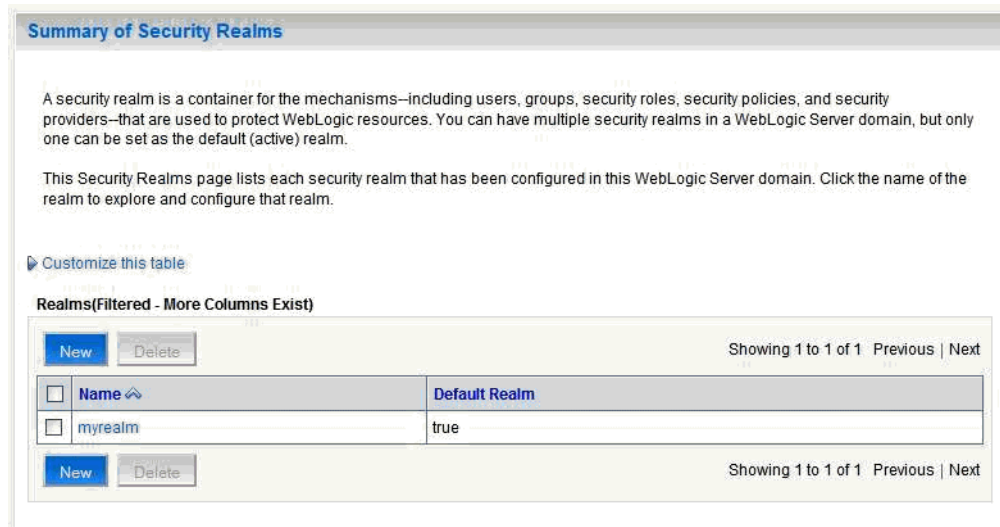
1. Log in to the WLS Administration Console.

For information on logging into the WLS Administration Console, see [Section 1.12.2, "Oracle WebLogic Server Administration Console"](#).

- From the Domain Structure pane, click **Security Realms**.

The Summary of Security Realms pane displays (see [Figure 14–62](#)).

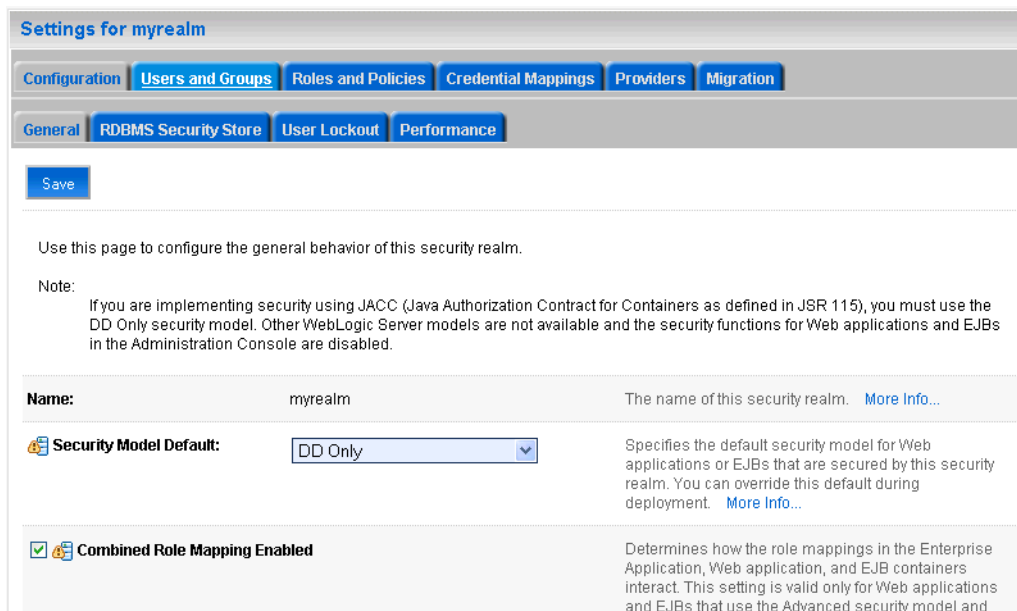
**Figure 14–62 Summary of Security Realms Pane**



- Click the realm entry for which to configure the OAM authenticator.

The Settings pane for the realm displays (see [Figure 14–63](#)).

**Figure 14–63 Settings Pane**



- Open the Providers tab.

The Provider Settings display (see [Figure 14–64](#)).

**Figure 14–64 Settings Pane - Providers**

Settings for myrealm

Configuration Users and Groups Roles and Policies Credential Mappings **Providers** Migration

Authentication Authorization Adjudication Role Mapping Auditing Credential Mapping Certification Path Keystores

An Authentication provider allows WebLogic Server to establish trust by validating a user. You must have one Authentication provider in a security realm, and you can configure multiple Authentication providers in a security realm. Different types of Authentication providers are designed to access different data stores, such as LDAP servers or DBMS. You can also configure a Realm Adapter Authentication provider that allows you to work with users and groups from previous releases of WebLogic Server.

Customize this table

**Authentication Providers**

New Delete Reorder Showing 1 to 2 of 2 Previous | Next

| <input type="checkbox"/> | Name                    | Description                          | Version |
|--------------------------|-------------------------|--------------------------------------|---------|
| <input type="checkbox"/> | DefaultAuthenticator    | WebLogic Authentication Provider     | 1.0     |
| <input type="checkbox"/> | DefaultIdentityAsserter | WebLogic Identity Assertion provider | 1.0     |

New Delete Reorder Showing 1 to 2 of 2 Previous | Next

5. Click **New** to create a new provider.

The Create a New Authentication Provider pane displays (see [Figure 14–65](#)).

**Figure 14–65 Create a New Authentication Provider Pane**

Create a New Authentication Provider

OK Cancel

**Create a new Authentication Provider**

The following properties will be used to identify your new Authentication Provider.

\* Indicates required fields

The name of the authentication provider.

\* **Name:**

This is the type of authentication provider you wish to create.

**Type:**  ▼

OK Cancel

6. Enter a name for the new provider (for example, `OID Authenticator`), select `OracleInternetDirectoryAuthenticator` as its type and click **OK**.
7. On the Providers tab, click the newly added provider.

The Common Settings pane for the authenticator displays (see [Figure 14–66](#)).

**Figure 14–66 Common Settings Pane**

The screenshot shows the 'Settings for OID Authenticator' configuration pane. At the top, there are two tabs: 'Configuration' and 'Performance'. Under 'Configuration', there are two sub-tabs: 'Common' (which is selected) and 'Provider Specific'. Below the sub-tabs is a 'Save' button. A message reads: 'Use this page to define the general configuration of this Oracle Internet Directory Authentication provider.' Below this is a table of configuration items:

|                      |  |   |
|----------------------|--|---|
| <b>Name:</b>         | OID Authenticator                          | The name of this Oracle Internet Directory Authentication provider. <a href="#">More Info...</a>                                |
| <b>Description:</b>  | Provider that performs LDAP authentication | A short description of this Oracle Internet Directory Authentication provider. <a href="#">More Info...</a>                     |
| <b>Version:</b>      | 1.0  | The version number of this Oracle Internet Directory Authentication provider. <a href="#">More Info...</a>                      |
| <b>Control Flag:</b> | <input type="text" value="SUFFICIENT"/>    | Specifies how this Oracle Internet Directory Authentication provider fits into the login sequence. <a href="#">More Info...</a> |

At the bottom of the pane is another 'Save' button.

8. Set the control flag to SUFFICIENT and click **Save**.
9. Open the Provider Specific tab.

The Provider Specific Settings pane for the authenticator displays (see [Figure 14–67](#)).

Figure 14–67 Provider Specific Settings for OID Authenticator

The screenshot shows the 'Settings for OID Authenticator' configuration page. It has two main tabs: 'Configuration' and 'Performance'. Under 'Configuration', there are sub-tabs for 'Common' and 'Provider Specific'. A 'Save' button is located at the top left. Below the tabs, there is a 'Save' button and a paragraph: 'Use this page to define the provider specific configuration for this Oracle Internet Directory Authentication provider.' The page is divided into two sections: 'Connection' and 'Users'.  
**Connection Section:**  
 - **Host:** localhost (The host name or IP address of the LDAP server. [More Info...](#))  
 - **Port:** 389 (The port number on which the LDAP server is listening. [More Info...](#))  
 - **Principal:** (The Distinguished Name (DN) of the LDAP user that WebLogic Server should use to connect to the LDAP server. [More Info...](#))  
 - **Credential:** (The credential (usually a password) used to connect to the LDAP server. [More Info...](#))  
 - **Confirm Credential:** (Empty field)  
 - **SSL Enabled:**  (Specifies whether the SSL protocol should be used when connecting to the LDAP server. [More Info...](#))  
**Users Section:**  
 - **User Base DN:** ou=people, o=example (The base distinguished name (DN) of the tree in the LDAP directory that contains users. [More Info...](#))  
 - **All Users Filter:** (&(cn=\*)(objectclass=pe) (An LDAP search filter for finding all users beneath the base user distinguished name (DN). Note: If you change the user name attribute to a type other than cn, you must duplicate that change in the User From Name Filter and User Name Attribute attributes. [More Info...](#))  
 - **User From Name Filter:** (&(cn=%u)(objectclass=) (An LDAP search filter for finding a user given the name of the user. The user name attribute specified in this filter must match the one specified in the All Users Filter and User Name Attribute attributes. [More Info...](#))  
 - **User Search Scope:** subtree (Specifies how deep in the LDAP directory tree the LDAP Authentication provider should search for users. [More Info...](#))  
 - **User Name Attribute:** cn (The attribute of an LDAP user object class that specifies the name of the user. The user name attribute specified must match the one specified in ...)

10. Complete the fields as shown in the table below. Leave the rest of the fields set to their default values.

| Field               | Value      | Comment   |
|---------------------|------------|---|
| Host:               |            | The host ID for the LDAP server   |
| Port:               |            | The LDAP server port number   |
| Principal:          |            | The LDAP administrator principal (for example, cn=orcladmin)                    |
| Credential:         | <password> | The administrator principal password  |
| Confirm Credential: | <password> |   |
| User Base DN:       |            | User Search Base - this value would be same as #1.d in OAM Access Manager Setup |

| Field                | Value                            | Comment                                  |
|----------------------|----------------------------------|--|
| All Users Filter:    | "(&(uid=*)(objectclass=person))" |  |
| User Name Attribute: | "uid"                            |  |
| Group Base DN:       |                                  | Group search base - Same as User Base DN |

11. Click **Save**.

12. Restart the WebCenter Administration Server and managed server and validate the configuration by navigating to the Realm Settings page in the WLS Administration Console and opening the Users and Groups tab.

#### 14.7.1.6.2 Configuring the OAM Identity Asserter

An OAM identity asserter needs to be configured with the provider Control Flag set to REQUIRED.

To configure the OAM Identity asserter:

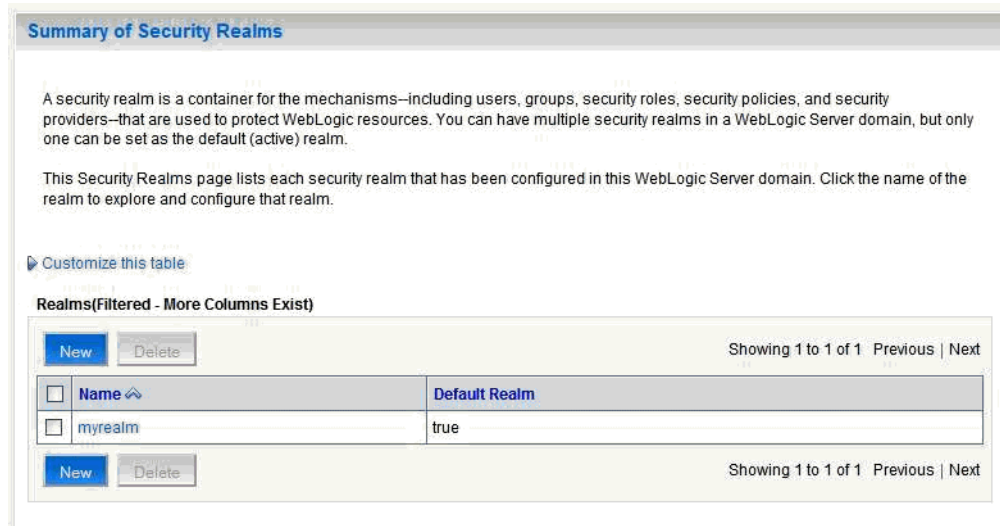
1. Log in to the WLS Administration Console.

For information on logging into the WLS Administration Console, see [Section 1.12.2, "Oracle WebLogic Server Administration Console"](#).

2. From the Domain Structure pane, click **Security Realms**.

The Summary of Security Realms pane displays (see [Figure 14–68](#)).

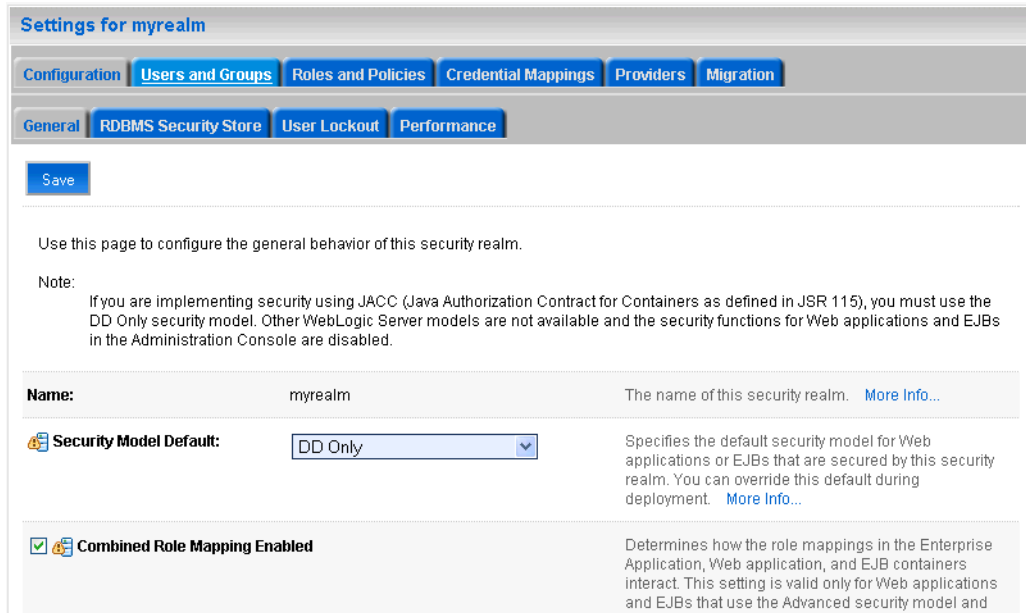
**Figure 14–68 Summary of Security Realms Pane**



3. Click the realm entry for which to configure the OAM identity asserter.

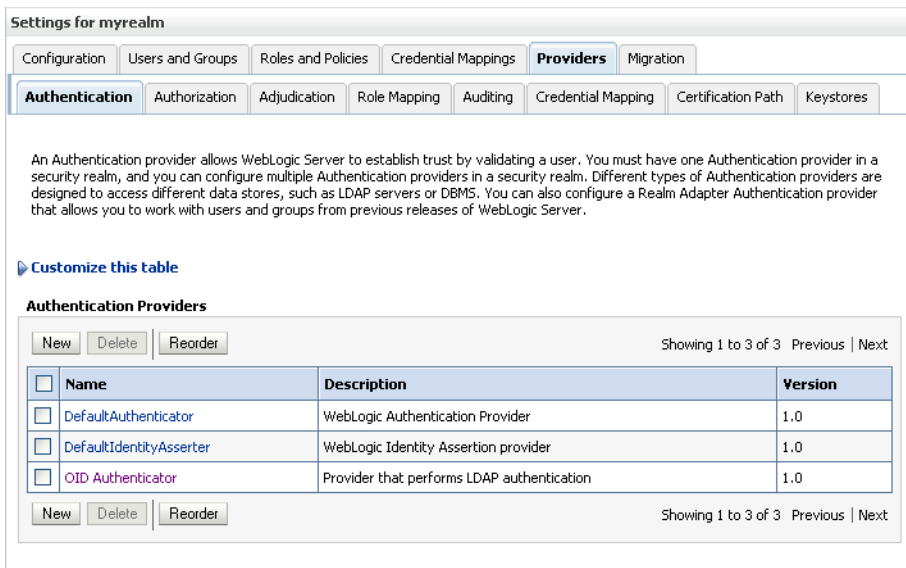
The Settings pane for the realm displays (see [Figure 14–69](#)).

**Figure 14–69 Settings Pane**



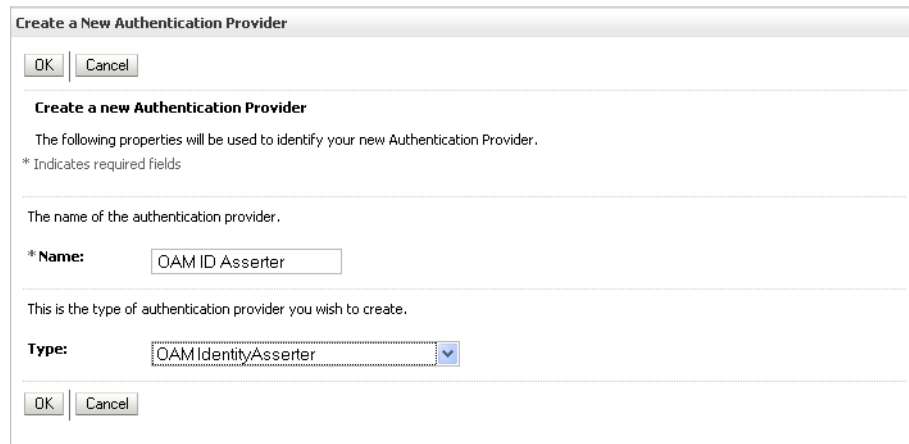
4. Open the Providers tab.  
The Provider Settings display (see [Figure 14–70](#)).

**Figure 14–70 Settings Pane - Providers**



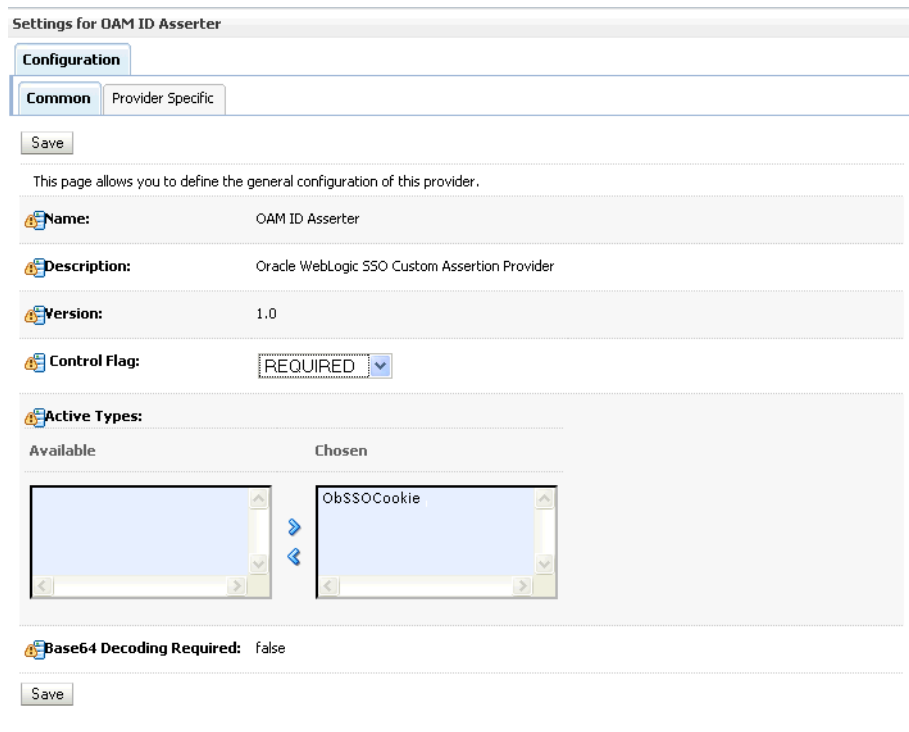
5. Click **New** to create a new provider.  
The Create a New Authentication Provider pane displays (see [Figure 14–71](#)).

**Figure 14–71 Create a New Authentication Provider Pane**



6. Enter a name for the new provider (for example, OAM ID Asserter), select OAMIdentityAsserter as its type and click **OK**.
7. On the Providers tab, click the newly added provider.  
The Common Settings pane for the authenticator displays (see [Figure 14–72](#)).

**Figure 14–72 Common Settings Pane**



8. Set the control flag to **REQUIRED** and check that `ObSSOCookie` is set for **Active Types**.
9. Click **Save**.
10. Open the **Provider Specific** tab.



The Provider Specific Settings pane for the OAMIdentityAsserter displays (see Figure 14-73).

**Figure 14-73 Provider Specific Settings for the OAMIdentityAsserter**

11. Complete the fields as shown in the table below. Leave the rest of the fields set to their default values.

| Field                  | Value | Comment  |
|------------------------|-------|--|
| Primary Access Server: |       | The OAM server endpoint information in HOST:PORT format          |
| Access Gate Name:      |       | Name of the Access Gate  |
| Access Gate Password:  |       | Provide the Access Gate password and confirm in the field below. |

12. Click **Save** to save your settings.

### 14.7.1.6.3 Configuring the Default Authenticator and Setting the Provider Order

After configuring the OAM identity asserter, make sure that the default authenticator's control flag is set to `SUFFICIENT` and reorder the providers as shown below:

1. Navigate to the Provider Settings pane (see [Figure 14-70](#)).
2. Open the Default Authenticator and check that the control flag is set to `SUFFICIENT`.
3. Do the same for any providers other than the two you just created.
4. On the Settings Pane, reset the provider order to:
  - `OAMIdentityAsserter (REQUIRED)`
  - `OracleInternetDirectoryAuthenticator (SUFFICIENT)`
  - `DefaultAuthenticator (SUFFICIENT)`
  - `DefaultIdentityAsserter`

#### 14.7.1.6.4 Configuring the Application for Oracle Access Manager SSO

Configure the applications for SSO by adding a setting to `EXTRA_JAVA_PROPERTIES`.

There is a system property that tells WebCenter and ADF that the application is configured in SSO mode and some special handling is required. The following system property is required in this mode:

| Field                                     | Value             | Comment  |
|---|-------------------|--|
| <code>oracle.webcenter.spaces.osso</code> | <code>true</code> | This flag tells WebCenter that SSO is being used, so no login form should be displayed on the default landing page. Instead, it will render a login link that the user can click to invoke the SSO authentication. |

To set this property, edit the `setDomainEnv.sh` script located in your `<domain>/bin` directory. Add the property to the `EXTRA_JAVA_PROPERTIES` variable, as follows:

```
EXTRA_JAVA_PROPERTIES="-Dweblogic.security.SSL.ignoreHostnameVerification=true
-Doracle.mds.bypassCustRestrict=true
-Djps.update.subject.dynamic=true -Doracle.webcenter.spaces.osso=true
-noverify ${EXTRA_JAVA_PROPERTIES}"
```

After making this change, restart the following servers:

- WebCenter's Administration Server
- All the domain's managed servers
- WebTier OHS

#### 14.7.1.7 Additional Configurations

The following configurations may be necessary or helpful in providing additional security for your site:

- [Configuring the WLS Administration Console and Enterprise Manager](#)
- [Configuring the Discussions Server](#)
- [Configuring the Wiki Server](#)
- [Restricting Access with Connection Filters](#)

### 14.7.1.7.1 Configuring the WLS Administration Console and Enterprise Manager

This section describes how to optionally set up OAM single sign-on for the WLS Administration Console and Enterprise Manager.

---

**Note:** Setting up OAM SSO for Enterprise Manager and the WLS Administration Console would provide single sign-on access to same set of users for whom OAM SSO access has been configured. If want the Webtier to be accessible to external users through OAM, but want administrators to log in directly to Enterprise Manager and the WLS Administration Console, then you may not want to complete this additional configuration step.

---

To set up OAM SSO for the WLS Administration Console and Enterprise Manager:

1. Log in to the Access Server Console using your browser to navigate to:

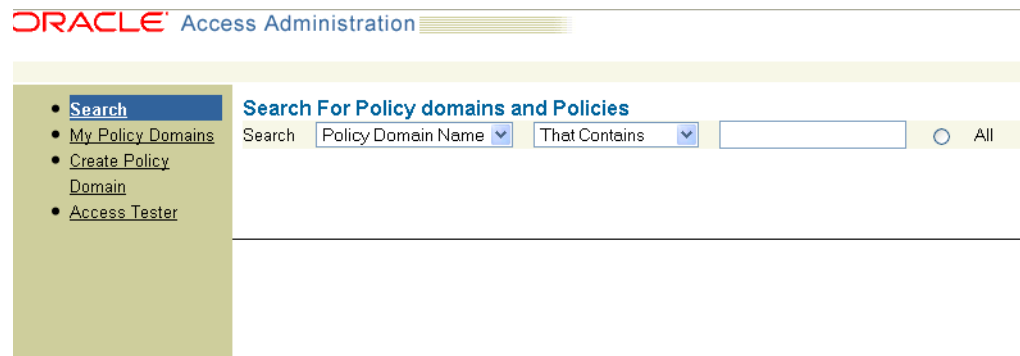
`http://host:port/access/oblix`

Where *host* is the host ID of the server hosting the Access Manager (for example, `oam.example.com`), and *port* is the HTTP port number (for example, 8888).

2. Click **Policy Manager**.

The Policy Manager pane displays (see [Figure 14-74](#)).

**Figure 14-74 Policy Manager Pane**



3. Search for the policy domain that you created earlier to protect WebCenter resources in [Section 14.7.1.5, "Manually Defining the WebCenter Policy Domain"](#).
4. Open the Resources tab and click **Add**.  
The Resource page displays (see [Figure 14-75](#)).

**Figure 14–75 Policy Domain Resource Page**

webtier.example.com  
[MyPolicyDomain](#) > [Resource](#)

General Resources Authorization Rules Default Rules Policies Delegated Access Admins

Resource Type

---

Host Identifiers

URL Prefix

Description

Update Cache

5. Add the resources that need to be secured. For each resource:
  - a. Select `http` as the **Resource Type**.
  - b. Select the **Host Identifier** for the WebCenter webtier.
  - c. Enter the **URL Prefix** for the WLS Administration Console or Enterprise Manager.
  - d. Enter a **Description** for the resource.
  - e. Make sure that **Update Cache** is selected, and then click **Save**.
6. In your webtier, modify the `mod_wl_ohs.conf` file (in `WEBTIER_HOME/instances/your_instance/config/OHS/ohs1/`) to include the WLS Administration Console and Enterprise Manager, using the actual host ID for the WebCenter Administration Server for WebLogicHost.

```
<IfModule mod_weblogic.c>
  MatchExpression /webcenter
  WebLogicHost=example.com|WebLogicPort=8888
  MatchExpression /rss
  WebLogicHost=example.com|WebLogicPort=8888
  MatchExpression /owc_wiki
  WebLogicHost=example.com|WebLogicPort=8890
  MatchExpression /owc_discussions
  WebLogicHost=example.com|WebLogicPort=8890
  MatchExpression /console
  WebLogicHost=example.com|WebLogicPort=7001
  MatchExpression /em
  WebLogicHost=example.com|WebLogicPort=7001
</IfModule>
```

7. Restart the Oracle HTTP Server for your changes to take effect.

You should now be able to access the WLS Administration Console and Enterprise Manager with the following links:

```
http://host:OHS port/console
http://host:OHS port/em
```

and be prompted with the OAM SSO login form.

### 14.7.1.7.2 Deploying the Discussions Server

Prior to configuring the Oracle WebCenter Discussions Server for SSO, you may need to deploy it.

To deploy the discussions server:

1. Log into the WLS Administration Console.

For information on logging into the WLS Administration Console, see [Section 1.12.2, "Oracle WebLogic Server Administration Console"](#).

2. In the Domain Structure pane, click **Deployments**.

The Deployments Summary pane displays (see [Figure 14–76](#)).

**Figure 14–76** *Deployment Summary Pane*

**Summary of Deployments**

**Control** Monitoring

This page displays a list of Java EE applications and stand-alone application modules that have been installed to this domain. Installed applications and modules can be started, stopped, updated (redeployed), or deleted from the domain by first selecting the application name and using the controls on this page.

To install a new application or module for deployment to targets in this domain, click the Install button.

[Customize this table](#)

**Deployments**

Install Update Delete Start Stop Showing 1 to 35 of 35 Previous Next

| <input type="checkbox"/> | Name                                      | State  | Health | Type                   | Deployment Order |
|--------------------------|---|--------|--------|------------------------|------------------|
| <input type="checkbox"/> | adf.oracle.domain(1.0,11.1.1.1.0)         | Active |        | Library                | 100              |
| <input type="checkbox"/> | adf.oracle.domain.webapp(1.0,11.1.1.1.0)  | Active |        | Library                | 100              |
| <input type="checkbox"/> | custom.webcenter.spaces(11.1.1,11.1.1)    | Active |        | Library                | 300              |
| <input type="checkbox"/> | DMS Application (11.1.1.1.0)              | Active | OK     | Web Application        | 190              |
| <input type="checkbox"/> | FMW Welcome Page Application (11.1.0.0.0) | Active | OK     | Web Application        | 150              |
| <input type="checkbox"/> | jpdck                                     | Active | OK     | Enterprise Application | 100              |

3. On the Deployment Summary page, select `owc_discussions` stop and delete and click **Install**.
4. Using the Install Application Assistant **Path** field, locate the SSO enabled `owc_discussions` .EAR file (typically in `MW_HOME/Oracle_WC1/discussionserver`).
5. Select the `owc_discussions_sso.ear` file and click **Next**.
6. Select **Install this deployment as an application** and click **Next**.
7. Deploy the .EAR file with all default options except the **Name**, which should be set to `owc_discussions`.
8. Restart the `WLS_Services` managed server.

Now, when you access the discussion server's Admin Console through the OHS port:

```
http://<host>:<OHS port>/owc_discussions/admin/
```

you should be challenged by the WebGate login form.

#### 14.7.1.7.3 Configuring the Discussions Server

This section describes how to configure Oracle WebCenter Discussions Server for OAM single sign-on. Before configuring the discussions server for OAM SSO, deploy it as shown in [Section 14.7.1.7.2, "Deploying the Discussions Server"](#), and configure it to use the same identity store LDAP as WebCenter Spaces, as described in [Section 14.3.6, "Configuring the Discussions Server to Share the Identity Store LDAP Server"](#).

##### To set up the discussions server for OAM SSO

1. Log in to the Oracle WebCenter Discussions Server Admin Console at:

```
http://host:port/owc_discussions/admin
```

Where *host* and *port* are the host ID and port number of the WLS\_Services managed server.

2. Open the System Properties page and edit (if it already exists) or add the `AuthFactory.className` property setting it's value to `oracle.jive.sso.OracleSSOAuthFactory`.
3. Edit or add the `jiveURL` property to point to the base URL of the SSO server. For example:

```
jiveURL = example.com:8890/owc_discussions
```

4. Deploy the SSO-enabled `owc_discussions` application.

##### To create a discussions server connection for WebCenter Spaces

1. Log into Fusion Middleware Control and select the WebLogic domain for WebCenter Spaces.

For information on logging into Fusion Middleware Control, see [Section 6, "Starting Enterprise Manager Fusion Middleware Control"](#).

2. In the Navigation pane, open the WebCenter node, and then the WebCenter Spaces node, and click `WebCenter Spaces (WLS_Spaces)`.
3. Register the discussion server as described in [Section 11.1.3.1, "Registering Discussion Servers Using Fusion Middleware Control"](#).

For **Server URL**, enter `http://<host>:<port>/owc_discussions`.

4. Restart the `WLS_Spaces` managed server.

When you log into WebCenter Spaces, you automatically sign on to the discussion server as well.

#### 14.7.1.7.4 Configuring the Wiki Server

Wiki page functionality is supported as a portlet, which you can embed in a Web page, and OAM single sign-on is supported this way. Since the Oracle WebCenter Wiki and Blog Server does not require or support an identity store, there is no need to configure the LDAP.

To add a wiki page to a WebCenter identity store, follow the steps below:

1. Log in to WebCenter Spaces, and open a group space.
2. Add a page, choosing `Web Page` as the **Style**.
3. When the page is created, click the **Edit** icon.

The Component properties dialog displays.

4. Enter the following URL in the **Source** box:

```
http://host:OHS_port/owc_
wiki/page/show.jz?inline=1&scope=#{communityContext.communityName}
```

Where *host* is the host ID of the `WLS_Spaces` server, and *OHS\_port* is the port number of the Oracle HTTP Server. The OHS port is used so the call goes through the WebGate which will initiate SSO.

After specifying the component properties you will see the wiki page contents.

5. Save the changes.

#### 14.7.1.7.5 Restricting Access with Connection Filters

Follow the steps below to only allow users to access WebCenter and other services through the WebTier OHS ports so that they can be properly authenticated.

1. Log in to the WLS Administration Console.

For information on logging into the WLS Administration Console, see [Section 1.12.2, "Oracle WebLogic Server Administration Console"](#).

2. In the Domain Structure pane, select the domain you want to configure (for example, `webcenter`).

3. Open the Security tab and the Filter subtab.

The Security Filter Settings pane displays (see [Figure 14-77](#)).

**Figure 14-77 Security Filter Settings Page**

Settings for webcenter

Configuration Monitoring Control **Security** Web Service Security Notes

General **Filter** Unlock User Embedded LDAP Roles Policies

Save

This page allows you to define connection filter settings for this WebLogic Server domain.

**Connection Logger Enabled** Specifies whether this WebLogic Server domain should log accepted connections. [More Info...](#)

**Connection Filter:**  The name of the Java class that implements a connection filter (that is, the `weblogic.security.net.ConnectionFilter` interface). If no class name is specified, no connection filter will be used. [More Info...](#)

**Connection Filter Rules:**  The rules used by any connection filter that implements the `ConnectionFilterRulesListener` interface. When using the default implementation and when no rules are specified, all connections are accepted. The default implementation rules are in the format: `target localAddress localPort action protocols`. [More Info...](#)

Save

4. Check **Connection Logger Enabled** to enable the logging of accepted messages.

The Connection Logger logs successful connections and connection data in the server. This information can be used to debug problems relating to server connections.

5. In the **Connection Filter** field, specify the connection filter class to be used in the domain.
  - To configure the default connection filter, specify `weblogic.security.net.ConnectionFilterImpl`.
  - To configure a custom connection filter, specify the class that implements the network connection filter. Note that this class must also be present in the CLASSPATH for WebLogic Server.
6. In the Connection Filter Rules field, enter the syntax for the connection filter rules.

For example:

```
<webtier IP>/0 * * allow
0.0.0.0/0 * * deny
```

which says: allow all traffic coming from the local host and disallow all traffic from any other IP address. You should, of course, write the network filter(s) that are relevant to your environment. For more information about writing connection filters, see "Developing Custom Connection Filters" in *Oracle Fusion Middleware Programming Security for Oracle WebLogic Server*.

7. Click **Save** and activate the changes.
8. Restart all the managed servers and the Administration Server.
9. Verify that all direct traffic to the WLS server is blocked by attempting to navigate to:

```
http://host:WLS_port/webcenter
```

This should produce the following error:

```
"The Server is not able to service this request:
[Socket:000445]Connection rejected, filter blocked Socket,
weblogic.security.net.FilterException: [Security:090220]rule
3"
```

You should, however, still be able to access WebCenter through the OHS port:

```
http://host:OHS_port/webcenter
```

## 14.7.2 Configuring Oracle Single Sign-On (OSSO)

In a default installation, WebCenter uses the HTTP ports in the WLS managed server created for WebCenter. To configure WebCenter with Oracle Single Sign-On, WebCenter needs Oracle HTTP Server and the associated Module `mod_osso` to integrate with Oracle Single Sign-On (OSSO).

---

---

**Note:** The BPEL Console does not support SSO integration. When WebCenter is configured for SSO, login to BPEL must still be done through the standard login page on the BPEL Console.

---

---

This section includes the following subsections

- [OSSO Components and Topology](#)
- [Configuring the Oracle HTTP Server and Associated mods](#)
- [Configuring the OSSOIdentityAsserter](#)

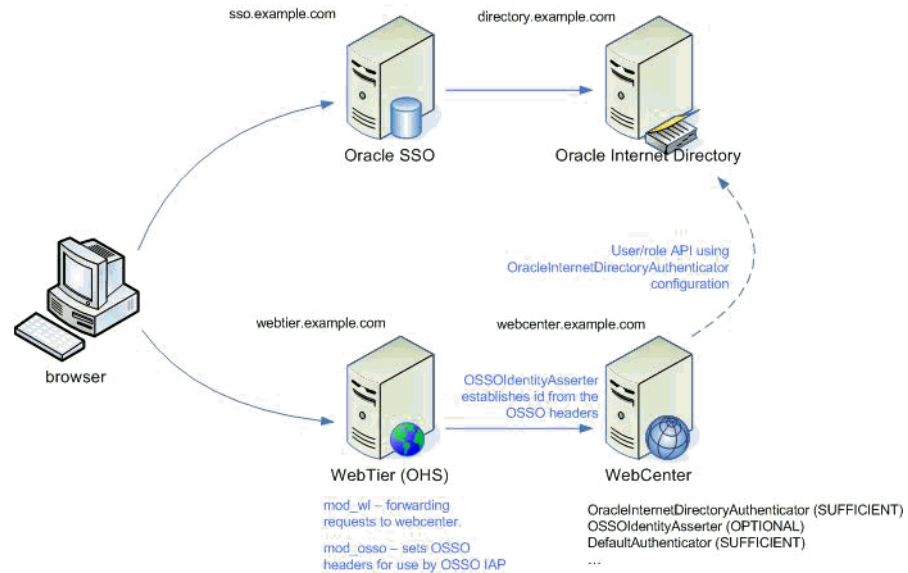


- [Registering OHS with Oracle SSO](#)

### 14.7.2.1 OSSO Components and Topology

In a default installation, WebCenter uses the HTTP ports of the WLS managed server created for WebCenter. To configure WebCenter with Oracle Single Sign-On, WebCenter needs the Oracle HTTP Server and the associated Module `mod_osso`, to integrate with Oracle SSO. The diagram below (Figure 14–78) shows the overall architecture of this integration:

**Figure 14–78 OSSO Components and Topology**



### 14.7.2.2 Configuring the Oracle HTTP Server and Associated mods

This section describes how to load and configure the Oracle HTTP Server and associated mods.

#### To load and configure the Oracle HTTP Server and associated mods

1. Install the WebTier, which contains Oracle HTTP Server (OHS) and associated mods (`mod_osso` and `mod_wl`).
2. Configure the module `mod_wl` in WebTier OHS so that it forwards requests to the Oracle WebLogic Server for WebCenter.

Uncomment the lines at `WEBTIER_HOME/instances/your_instance/config/OHS/ohs1/mod_wl_ohs.conf`. This file is included by the `httpd.conf` file and looks like the following:

```
LoadModule weblogic_module    ORACLE_HOME/ohs/modules/mod_wl_22.so
<IfModule mod_weblogic.c>
MatchExpression /webcenter WebLogicHost=webcenter.example.com|WebLogicPort=8888
MatchExpression /rss WebLogicHost=webcenter.example.com|WebLogicPort=8890
MatchExpression /owc_wiki WebLogicHost=webcenter.example.com|WebLogicPort=8890
MatchExpression /owc_discussions
WebLogicHost=webcenter.example.com|WebLogicPort=8890
MatchExpression /workflow WebLogicHost=soa.example.com|WebLogicPort=8888
MatchExpression /integration WebLogicHost=soa.example.com|WebLogicPort=8888
</IfModule>
```

### 14.7.2.3 Configuring the OSSOIdentityAsserter

Include the OSSO Identity Assertion Provider (IAP) provider in the Oracle WebLogic domain for WebCenter. Use the WLS Administration Console to add the OSSO IAP to your domain as shown in the steps below.

To configure the OSSOIdentityAsserter:

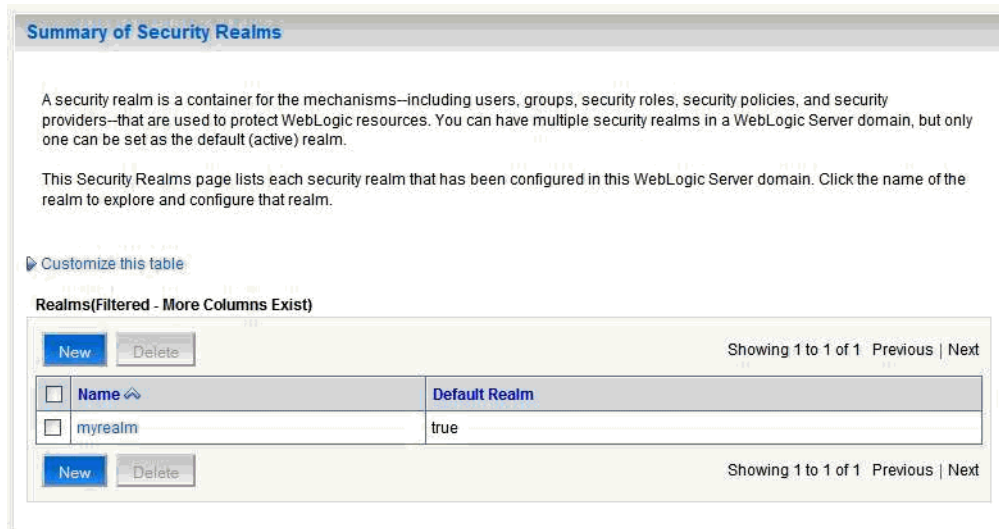
1. Log in to the WLS Administration Console.

For information on logging into the WLS Administration Console, see [Section 1.12.2, "Oracle WebLogic Server Administration Console"](#).

2. From the Domain Structure pane, click **Security Realms**.

The Summary of Security Realms pane displays (see [Figure 14–79](#)).

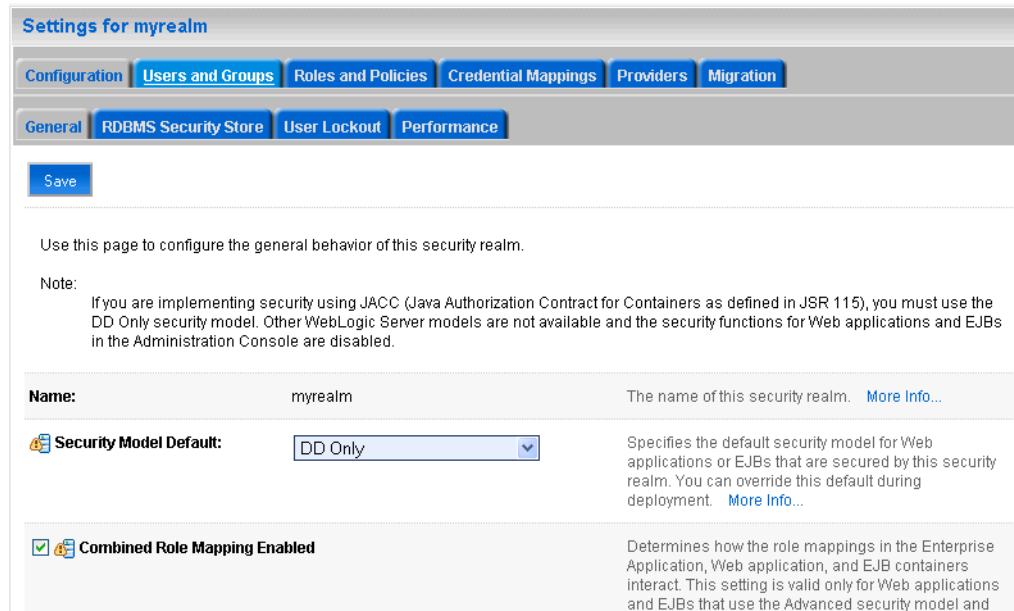
**Figure 14–79 Summary of Security Realms Pane**



3. Click the realm entry to which to add the provider.

The Settings pane for the realm displays (see [Figure 14–80](#)).

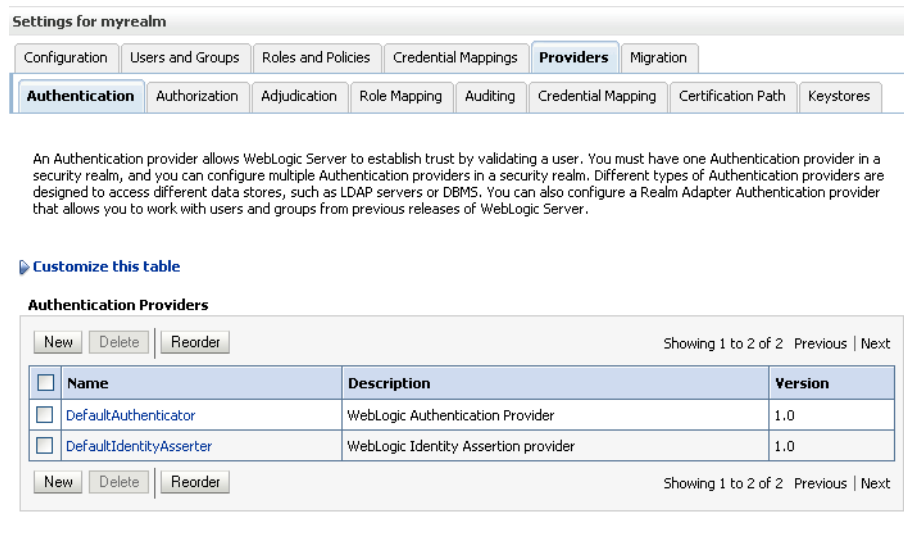
Figure 14–80 Settings Pane



4. Click the Providers tab.

The Provider Settings display (see [Figure 14–81](#)).

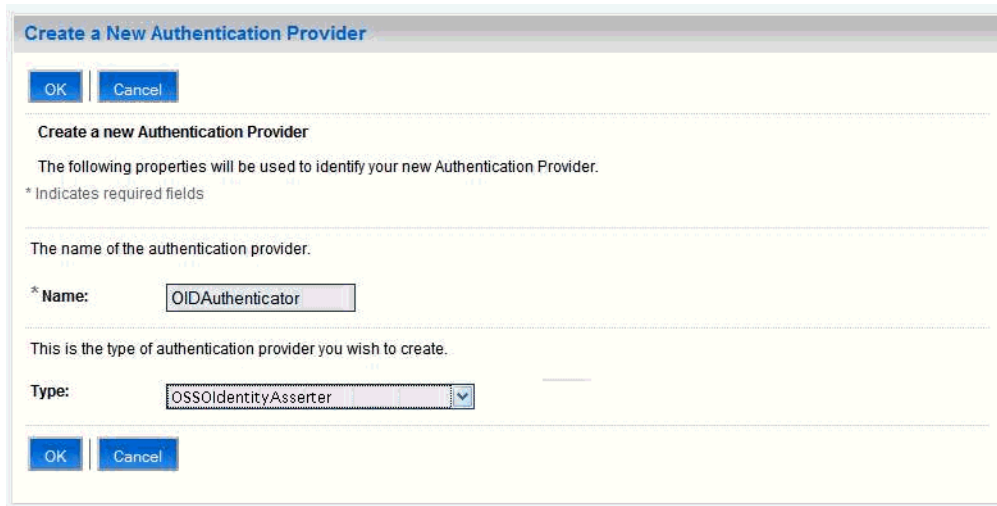
Figure 14–81 Settings Pane - Providers



5. Click New to create a new provider.

The Create a New Authentication Provider pane displays (see [Figure 14–82](#)).

**Figure 14–82 Create a New Authentication Provider Pane**



6. Enter a name for the new provider, select **OSSOIdentityAsserter** as its type and click **OK**.
7. On the Providers tab, click the newly added provider.
8. Set the control flag to **OPTIONAL**.
9. Make sure that **OracleInternetDirectoryAuthenticator** is set as the primary authenticator for the domain so that the user profile info can be obtained from the associated Oracle Internet Directory server.

The provider list should appear as follows:

- **OracleInternetDirectoryAuthenticator** (SUFFICIENT)
- **OSSOIdentityAsserter** (OPTIONAL)
- **DefaultAuthenticator** (SUFFICIENT)
- **DefaultIdentityAsserter** (OPTIONAL)

Also make sure that the default `jpsContext` in WebCenter's `jps-config.xml` file is set to the `idstore.ldap` serviceInstance.

10. Configure the Provider Specific details of the OSSO IAP with the settings for the following fields:

| Field                                | Value | Comment  |
|--------------------------------------|-------|--|
| LDAPPort                             |       | The LDAP port of the OID server  |
| Password                             |       | The password of the LDAP entry to be used for the connection (for example, <code>cn=orcladmin</code> , or other less privileged account) |
| Confirm Password                     |       | Re-enter the password to confirm.  |
| Admin DN                             |       | The account to be used for the connection  |
| Use Retrieved User Name As Principal | True  |  |
| Cache TTL                            | 60    |  |
| Rolefetching Enabled                 | False |  |

| Field                  | Value | Comment                         |
|------------------------|-------|---------------------------------|
| Level                  | 1     |                                 |
| Initial Cache Capacity | 128   |                                 |
| LDAPHost               |       | The host name of the OID server |
| Maximum Cache Capacity | 1024  |                                 |

#### 14.7.2.4 Registering OHS with Oracle SSO

Register the module `mod_osso` in the WebTier OHS with the SSO Server as a partner application by following the steps below.

To register OHS with Oracle SSO:

1. Run `ssoreg` from the SSO server to generate an `osso.conf` file and manually copy it to the partner application (`WEBTIER_HOME`).

This example shows how you would register a remote partner application on a SSO Server:

```
bash-3.00$ ORACLE_HOME/sso/bin/ssoreg.sh -site_name
webtier.example.com:80 -config_mod_osso TRUE -mod_osso_url
http://webtier.example.com -remote_midtier -config_file
webtier.example.com.osso.conf
```

Running this command creates a `webtier.example.com.osso.conf` file.

2. Copy the `WEBTIER_HOME/instances/your_instance/config/OHS/ohs1/disabled/mod_osso.conf` file to `WEBTIER_HOME/instances/your_instance/config/OHS/ohs1/moduleconf`. All files in the `moduleconf` directory are included in the `httpd.conf` file.
3. Add a static rule to the `mod_osso.conf` file to protect the `/webcenter` URL with Oracle SSO.

The `mod_osso.conf` file should look similar to this:

```
LoadModule osso_module ORACLE_HOME/ohs/modules/mod_osso.so
<IfModule mod_osso.c>
    OsoIpCheck off
    OsoIdleTimeout off
    OsoSecureCookies Off
```

# whatever the location of your real `osso.conf` file is, that was generated from the `ssoreg.sh` command.

```
OsoConfigFile /OracleWebTier/webtier.example.com.osso.conf
```

```
# _____
# Notes
# _____
# 1. Here's what you need to add to protect a resource,
#    e.g. <ApacheServerRoot>/htdocs/private:
# 2. if an application is protected by SSO then no matter what Apache will
always
#    send no-cache headers practically undoing whatever the Apache
configuration or
#    the ADF faces Cache library do. To allow caching for SSO protected
resources
#    add "OsoSendCacheHeaders off " as following.
```

```

<Location /webcenter/adfAuthentication>
  OssoSendCacheHeaders off
  require valid-user
  AuthType Osso
</Location>
<Location /owc_wiki/user/login.jz>
  OssoSendCacheHeaders off
  require valid-user
  AuthType Osso
</Location>
<Location /rss/rssservlet>
  OssoSendCacheHeaders off
  require valid-user
  AuthType Osso
</Location>
<Location /owc_discussions/login!withRedirect.jspa>
  OssoSendCacheHeaders off
  require valid-user
  AuthType Osso
</Location>
<Location /owc_discussions/login!default.jspa>
  OssoSendCacheHeaders off
  require valid-user
  AuthType Osso
</Location>
<Location /owc_discussions/login.jspa>
  OssoSendCacheHeaders off
  require valid-user
  AuthType Osso
</Location>
<Location /owc_discussions/admin>
  OssoSendCacheHeaders off
  require valid-user
  AuthType Osso
</Location>
<Location /owc_wiki/adfAuthentication>
  OssoSendCacheHeaders off
  require valid-user
  AuthType Osso
</Location>
<Location /integration/worklistapp>
  OssoSendCacheHeaders off
  require valid-user
  AuthType Osso
</Location>
<Location /workflow/WebCenterWorklistDetail>
  OssoSendCacheHeaders off
  require valid-user
  AuthType Osso
</Location>
<Location /workflow/sdpmessagingsca-ui-worklist>
  OssoSendCacheHeaders off
  require valid-user
  AuthType Osso
</Location>

</IfModule>
#
# If you would like to have short hostnames redirected to

```

```
# fully qualified hostnames to allow clients that need
# authentication via mod_osso to be able to enter short
# hostnames into their browsers uncomment out the following
# lines
#
#PerlModule Apache::ShortHostnameRedirect
#PerlHeaderParserHandler Apache::ShortHostnameRedirect
```

Be sure to change the **OsssoConfigFile** parameter to point to the location (and filename if you've changed it) of your `osso.conf` file.

4. Restart the WebTier so that the configuration changes to `mod_osso` and `mod_wl` to take effect.
5. For the Worklist service changes to take effect, run the following command on the WebCenter Administration server:

```
setBPPELConnection('webcenter', 'WebCenter-Worklist',
'http://webcenter-stage.example.com')
```

6. To only allow users to access WebCenter and other services through the WebTier OHS ports so that they can be properly authenticated, follow the steps in [Section 14.7.1.7.5, "Restricting Access with Connection Filters"](#).

### 14.7.3 Configuring SAML-based Single Sign-on

Security Assertion Markup Language (SAML) enables cross-platform authentication between Web applications or Web Services running in a WebLogic Server domain and Web browsers or other HTTP clients. WebLogic Server supports single sign-on (SSO) based on SAML. When users are authenticated at one site that participates in a single sign-on (SSO) configuration, they are automatically authenticated at other sites in the SSO configuration and do not need to log in separately.

This SSO mechanism can be used for departmental WebCenter installations for which there is no existing Oracle SSO or Oracle Access Manager single sign-on infrastructure, but single sign-on between only WebCenter Spaces and its services is required. For High Availability and large enterprise deployments, the Oracle Access Manager SSO configuration is recommended.

This section describes how to set up SAML 1.1-based single sign-on for Oracle WebCenter Spaces and the Wiki and Worklist services running on different managed servers within the same domain.

This section includes the following subsections:

- [SAML Components and Topology](#)
- [Configuring SAML-based Single Sign-on](#)

#### 14.7.3.1 SAML Components and Topology

[Figure 14–84](#) shows the components and their interaction in a SAML-based single sign-on configuration that includes WebCenter Spaces and the Wiki service.

A SAML-based single sign-on solution consists of the following components:

- **SAML Credential Mapper** - The SAML Credential Mapping provider acts as a producer of SAML security assertions, allowing WebLogic Server to act as a source site for using SAML for single sign-on. The SAML Credential Mapping provider generates valid SAML 1.1 assertions for authenticated subjects based on the configuration of the target site or resource.

- **Inter Site Transfer Service (ITS)** - an addressable component that generates identity assertions and transfers the user to the destination site.
- **Assertion Retrieval Service (ARS)** - an addressable component that returns the SAML assertion that corresponds to the artifact. The assertion ID must have been allocated at the time assertion was generated.
- **SAML Identity Asserter** - The SAML Identity Assertion provider acts as a consumer of SAML security assertions, allowing WebLogic Server to act as a destination site for using SAML for single sign-on. The SAML Identity Assertion provider processes valid SAML 1.1 assertions for authenticated subjects obtained from the source site or resource.
- **Assertion Consumer Service (ACS)** - an addressable component that receives assertions and/or artifacts generated by the ITS and uses them to authenticate users at the destination site
- **SAML Relying party** - A SAML Relying Party is an entity that relies on the information in a SAML assertion produced by the SAML source site. You can configure how WebLogic Server produces SAML assertions separately for each Relying Party or use the defaults established by the Federation Services source site configuration for producing assertion.
- **SAML Asserting party** - A SAML Asserting Party is a trusted SAML Authority (an entity that can authoritatively assert security information in the form of SAML Assertions).

Figure 14–83 shows the components and flow for a POST-configured SAML SSO configuration that includes both a WebCenter and SOA domain. The flow is similar for other destination applications participating in single sign-on such as RSS, Worklist applications, and Discussions.

**Figure 14–83 Detailed SAML Single Sign-on Components and Topology (POST Profile Configured)**

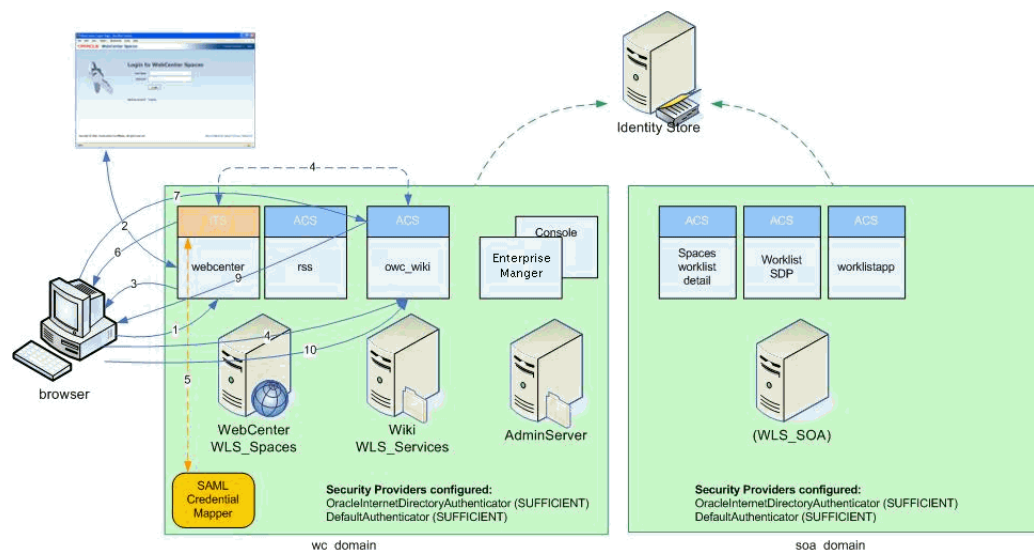
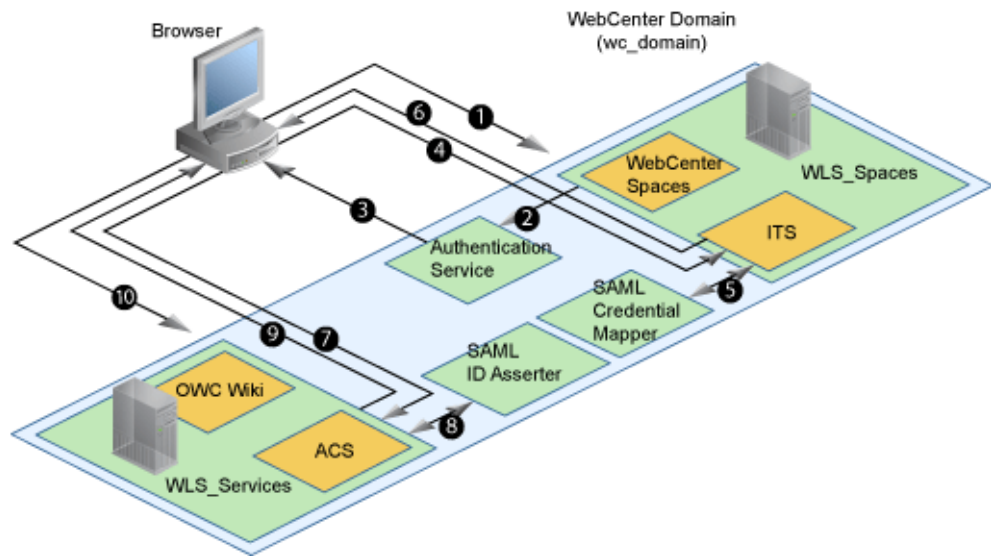


Figure 14–84 shows a simplified version of the components and flow for a POST-configured SAML SSO configuration, including the SAML SSO flow between WebCenter Spaces and the OWC Wiki application.



**Figure 14–84 SAML Single Sign-on Components and Topology (POST Profile Configured)**



The steps in the flow are:

1. The user's browser accesses WebCenter Spaces (source site), hosted on a WebLogic managed server (WLS\_Spaces) in the WebCenter domain (wc\_domain), by supplying user credentials.
2. WebCenter Spaces passes the user credentials to the authentication service provider.
3. If authentication is successful, the authenticated session is established, and the WebCenter Spaces welcome page is displayed.
4. From the welcome page, the user then clicks on a link on the page to access a secured Web page of the Wiki service (destination site), hosted on a different WebLogic Server (WLS\_Services) in the same domain. This triggers a call to the Inter-Site Transfer Service (ITS) servlet configured. In this case, the ITS servlet is hosted within the source site (that is, on the WebCenter Spaces application on the WLS\_Spaces managed server) that will share the same JSESSIONID cookie as WebCenter Spaces.
5. The ITS servlet calls the SAML Credential Mapper configured in the WebCenter domain (wc\_domain) to request a caller assertion. The SAML Credential Mapper returns the assertion. It also returns the URL of the destination site application Web page (a secured Web page of the Wiki service) and path to the appropriate POST form (if the source site is configured to use the POST profile).
6. The SAML ITS servlet generates a SAML response containing the generated assertion, signs it, base-64 encodes it, embeds it in the HTML form, and returns the form to the user's browser.
7. The user's browser POSTs the form to the destination site's Assertion Consumer Service (ACS). In this case, the ACS Servlet is hosted in destination site (the Wiki service) and shares its login cookie.
8. The assertion is validated.
9. If the assertion is successful, the user is redirected to the target (the secured Web page of the Wiki service).

10. The user is logged in on the destination site Wiki service without having to reauthenticate.

### 14.7.3.2 Configuring SAML-based Single Sign-on

Configuring SAML-based SSO consists of the following six steps:

- [Checking the Default WebCenter Spaces and Services Login](#)
- [Generating and Registering Certificates](#)
- [Creating the SAML Credential Mapping Provider Instance](#)
- [Configuring a Relying Party](#)
- [Configuring Source Site Federation Services](#)
- [Configuring the SAML Identity Assertion Provider](#)
- [Configuring Destination Site Federation Services](#)
- [Checking Your Configuration](#)
- [Configuring the Discussions Server for SAML SSO](#)

#### 14.7.3.2.1 Checking the Default WebCenter Spaces and Services Login

After installing WebCenter Spaces and the Wiki and Worklist services, you must test the single sign-on configuration.

To check the default WebCenter Spaces and Wiki service login:

1. Install WebCenter Spaces, and select the Wiki service and Discussions service, and any other service applications to be configured for SSO (RSS is automatically deployed when you install WebCenter Spaces). For information on installing WebCenter Spaces, see "Installing WebCenter Spaces, Portlet Producers, Discussions, and Wiki and Blogs" in the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter*.

When the installation is complete, WebCenter Spaces is hosted on the `WLS_Spaces` managed server, and Wiki and Discussions services are hosted on the `WLS_Services` managed server. Record the host and port that the Wiki service is running on so, later on, you can construct the URL and test single sign-on.

2. Log into WebCenter Spaces and create a personal page with a link to the Wiki service as shown below:
  - a. Log in to WebCenter Spaces as a user with create page permissions.
  - b. Create a new page by clicking on the **Create a page** tab in a group space.
  - c. Title the page appropriately (for example, "Wiki") and choose the Web page template.
  - d. Click the Inspector button and click on the Web page.
  - e. Change the source to be the URL specified below:

```
http://host:port/owc_
wiki/page/show.jz?inline=1&scope=#{communityContext.communityName}
```

Where *host* is the Wiki server host ID and *port* is the Wiki server port number.

- f. Save the page.

When you click the link, note that you are challenged to log in by the Wiki service. Once you have completed the remainder of the steps, this is not required. You will be automatically logged into Wiki service.

3. For the Worklist service, install SOA (which includes the BPEL server). For information on installing SOA, see *Oracle Fusion Middleware Installation Guide for Oracle SOA Suite*.
4. Configure the BPEL connection for WebCenter Spaces as described in [Section 11.5, "Setting Up Connections for the Worklist Service"](#).
5. To test the BPEL connection:
  - a. Log into WebCenter Spaces, create a group space, and add your administrator account as a moderator.
  - b. Log into WebCenter Spaces with your administrator account.  
You should see a new item in the Worklist task flow indicating that you have been added as a moderator for the group space.
  - c. Click the link.

Note that you are challenged to log in. After you have completed the rest of the steps you automatically log into the Worklist service on the SOA domain.

#### 14.7.3.2.2 Generating and Registering Certificates

Although optional, to secure communication between the SAML source and destination sites, communication should be encrypted. Additionally, certificates should be used to verify the identity of the other party during SAML interaction. Follow the steps below to generate a key using the `keytool` utility (available as part of the JDK 6.0), and register it using the WLS Administration Console.

##### To create certificates using keytool

1. Navigate to the `WEBLOGIC_HOME/server/lib` directory.
2. Using `keytool`, generate the key with the following command:

```
keytool -genkey -keypass key_password -keystore keystore_name -storepass keystore_password -keyalg rsa -alias alias
```

Where:

- `key_password` is the password to apply to the generated key
  - `keystore_name` is the name of the custom keystore
  - `keystore_password` is the password for the custom keystore
  - `alias` is the alias name (for example, `testalias`)
3. Run the `keytool` command with `-export` option to generate a key file calling it, for example, `testalias.der`.

```
keytool -export -keypass key_password -keystore keystore_name -storepass keystore_password -alias alias -file testalias.der
```

where:

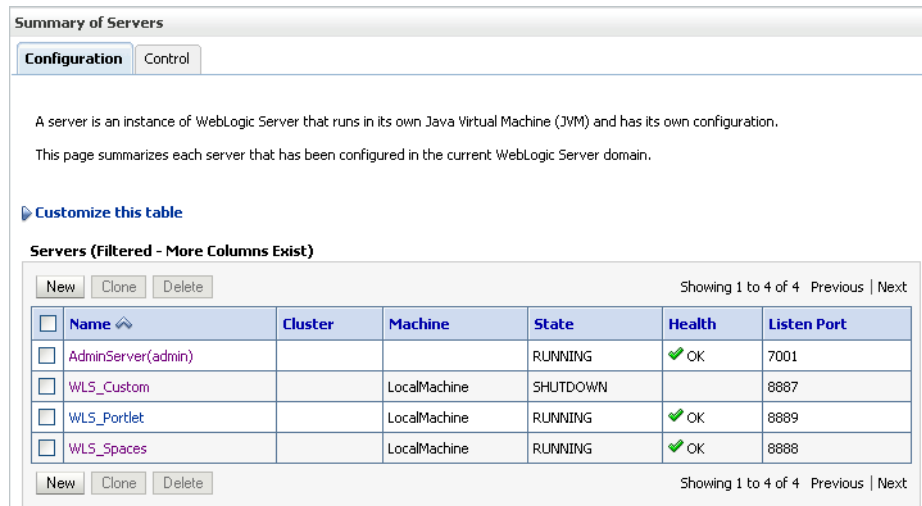
- `key_password` is the password for the generated key
- `keystore_name` is the name of the custom keystore
- `keystore_password` is the password for the custom keystore

- *alias* is the alias name (for example, *testalias*)

**To register the keystore using the WLS Administration Console**

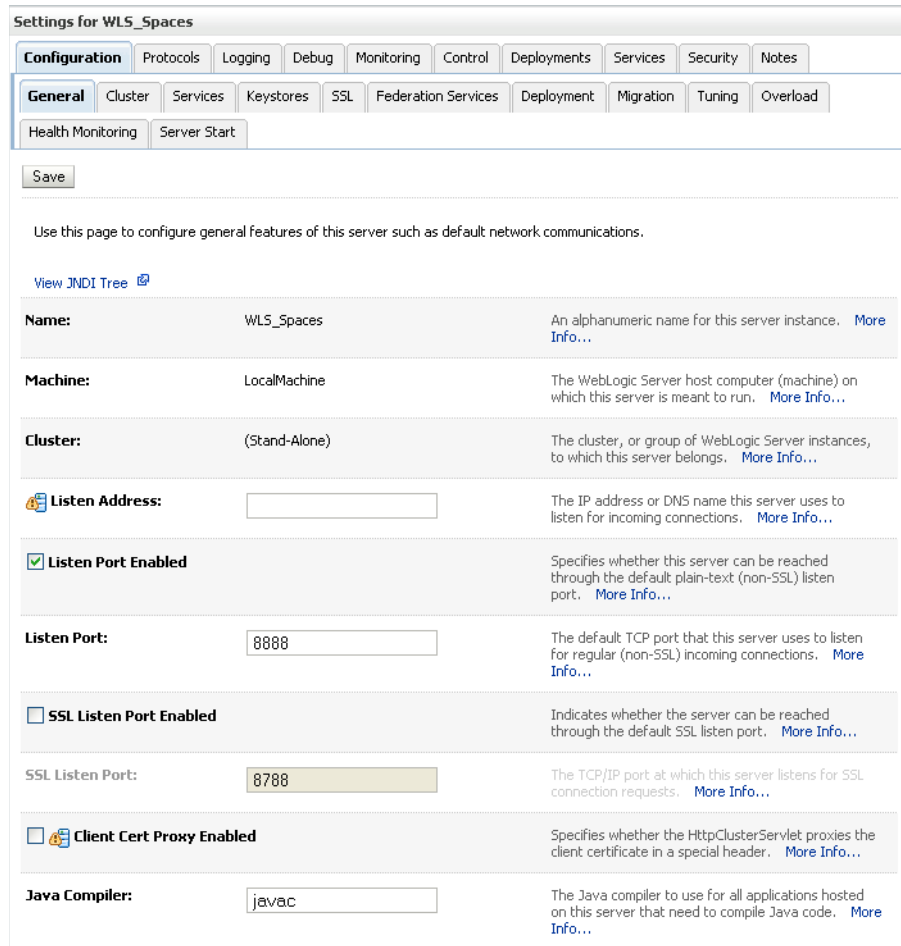
1. Log in to the WLS Administration Console.  
 For information on logging into the WLS Administration Console, see [Section 1.12.2, "Oracle WebLogic Server Administration Console"](#).
2. In the Domain Structure pane, expand **Environment** and click **Servers**.  
 The Summary of Servers pane displays (see [Figure 14–85](#)).

**Figure 14–85 Summary of Servers Pane**



3. Click the WebCenter Spaces server (*WLS\_Spaces*) to configure the identity and trust keystore.  
 The Settings pane for the WebCenter Spaces server displays (see [Figure 14–86](#)).

**Figure 14–86 Settings Pane for WebCenter Spaces Server**



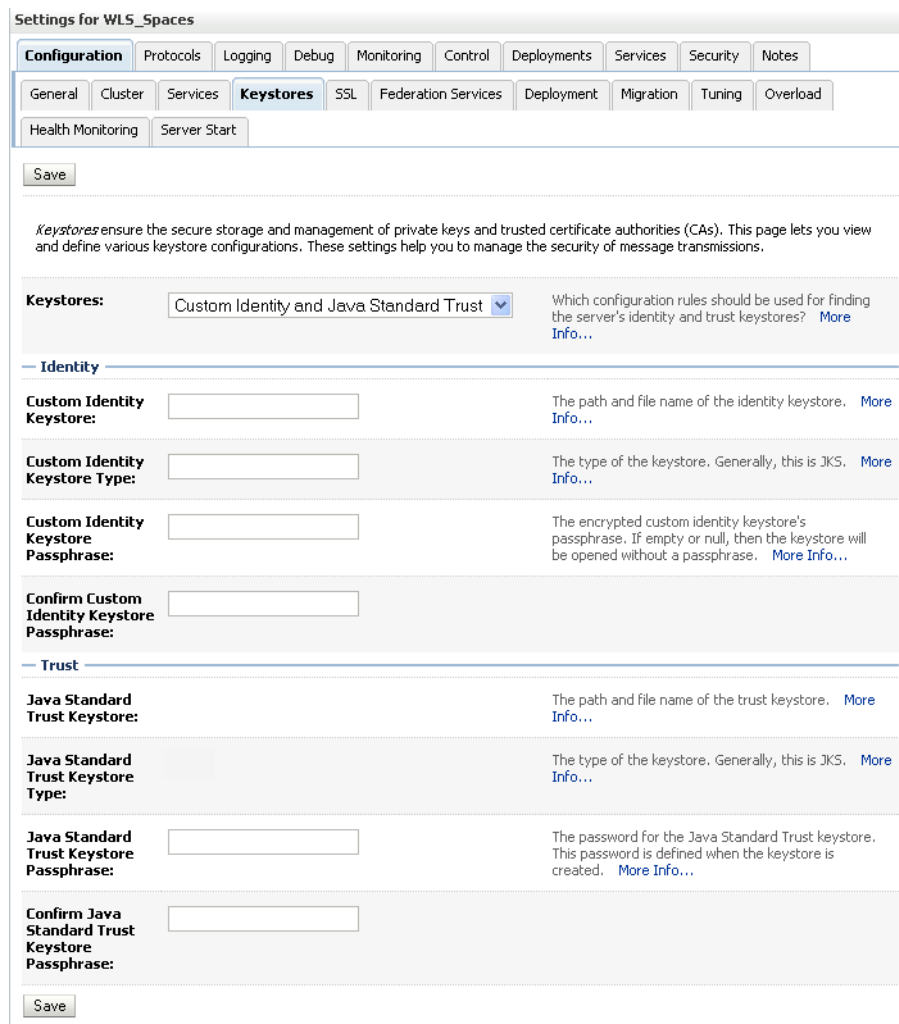
This screenshot shows the WLS Administration Console's Settings panel for the WebCenter Spaces server.

\*\*\*\*\*

4. Open the **Configuration** tab, and then the **Keystores** subtab.

The Keystores pane displays (see [Figure 14–87](#)).

**Figure 14–87 Keystores Pane**



5. For **Keystores**, select **Custom Identity and Java Standard Trust**.
6. In the **Identity** section, enter the path to the **Custom Identity Keystore** you created, choose **JKS** as the **Type**, and enter and confirm the **Custom Identity Keystore Passphrase**.
7. In the **Trust** section, enter the path to the trust keystore in **Java Standard Trust Keystore**, enter **JKS** as the **Type**, and enter and confirm the **Java Standard Trust Keystore Passphrase**.
8. Click **Save**.

#### 14.7.3.2.3 Creating the SAML Credential Mapping Provider Instance

This section describes how to create a SAML Credential Mapping Provider V2 instance. Note that the SAML Credential Mapping provider is not part of the default security realm and must be created.

Creating the SAML Credential Mapping Provider instance is the first of two steps required to configure the credential mapping provider:

- Creating the SAML Credential Mapping Provider instance

- Configuring a Relying Party for each of the participating service applications (which can include OWC Wiki, OWC Discussions, RSS, Worklist Community Detail, Worklist SDP, and Worklist Integration)

To create a SAML Credential Mapping Provider instance:

1. Log in to the WLS Administration Console.

For information on logging into the WLS Administration Console, see [Section 1.12.2, "Oracle WebLogic Server Administration Console"](#).

2. From the Domain Structure pane, click **Security Realms**.

The Summary of Security Realms pane displays (see [Figure 14–88](#)).

**Figure 14–88 Summary of Security Realms Pane**

**Summary of Security Realms**

A security realm is a container for the mechanisms—including users, groups, security roles, security policies, and security providers—that are used to protect WebLogic resources. You can have multiple security realms in a WebLogic Server domain, but only one can be set as the default (active) realm.

This Security Realms page lists each security realm that has been configured in this WebLogic Server domain. Click the name of the realm to explore and configure that realm.

[Customize this table](#)

**Realms(Filtered - More Columns Exist)**

New Delete Showing 1 to 1 of 1 Previous | Next

| <input type="checkbox"/> | Name ↕  | Default Realm |
|--------------------------|---------|---------------|
| <input type="checkbox"/> | myrealm | true          |

New Delete Showing 1 to 1 of 1 Previous | Next

3. Click your security realm.

The Settings page for the security realm displays (see [Figure 14–89](#)).

**Figure 14–89 Security Realm Settings Page**

**Settings for myrealm**

Configuration **Users and Groups** Roles and Policies Credential Mappings Providers Migration

General **RDBMS Security Store** User Lockout Performance

Save

Use this page to configure the general behavior of this security realm.

Note:  
If you are implementing security using JACC (Java Authorization Contract for Containers as defined in JSR 115), you must use the DD Only security model. Other WebLogic Server models are not available and the security functions for Web applications and EJBs in the Administration Console are disabled.

**Name:** myrealm The name of this security realm. [More Info...](#)

**Security Model Default:** DD Only Specifies the default security model for Web applications or EJBs that are secured by this security realm. You can override this default during deployment. [More Info...](#)

**Combined Role Mapping Enabled** Determines how the role mappings in the Enterprise Application, Web application, and EJB containers interact. This setting is valid only for Web applications and EJBs that use the Advanced security model and that initialize roles from deployment descriptors. [More Info...](#)

**Use Authorization Providers to Protect JMX Access** Configures the WebLogic Server MBean servers to use the security realm's Authorization providers to determine whether a JMX client has permission to access an MBean attribute or invoke an MBean operation. [More Info...](#)

Advanced

Save

- Open the Providers tab and select the Credential Mapping subtab.  
The Credential Mapping pane displays (see [Figure 14–90](#)).

**Figure 14–90 Credential Mapping Pane**

**Settings for myrealm**

Configuration Users and Groups Roles and Policies Credential Mappings **Providers** Migration

Authentication Authorization Adjudication Role Mapping Auditing **Credential Mapping** Certification Path

Keystores

A Credential Mapping provider allows WebLogic Server to log into a remote system on behalf of a subject that has already been authenticated. You must have one Credential Mapping provider in a security realm, and you can configure multiple Credential Mapping providers in a security realm.

[Customize this table](#)

**Credential Mapping Providers**

New Delete Reorder Showing 1 to 1 of 1 Previous | Next

| <input type="checkbox"/> | Name                    | Description                          | Version |
|--------------------------|-------------------------|--------------------------------------|---------|
| <input type="checkbox"/> | DefaultCredentialMapper | WebLogic Credential Mapping Provider | 1.0     |

New Delete Reorder Showing 1 to 1 of 1 Previous | Next

- Click **New**.



The Create a New Credential Mapping Provider pane displays (see [Figure 14-91](#)).

**Figure 14-91 Create a New Credential Provider Pane**

**Create a New Credential Mapping Provider**

OK Cancel

**Create a new Credential Mapping Provider**

The following properties will be used to identify your new Credential Mapping Provider.  
\* Indicates required fields

The name of the Credential Mapping Provider.

\* **Name:**

This is the type of credential mapping provider you wish to create.

**Type:**

OK Cancel

6. Enter a **Name** for the provider, select the **Type** as `SAMLCredentialMapperV2`, and click **OK**.
7. On the Security Realm Settings page, click the provider you just created. The Settings page for the new provider displays (see [Figure 14-92](#)).

**Figure 14-92 Provider Settings Pane**

**Settings for myrealm**

Configuration Users and Groups Roles and Policies Credential Mappings **Providers** Migration

Authentication Authorization Adjudication Role Mapping Auditing **Credential Mapping** Certification Path

Keystores

A Credential Mapping provider allows WebLogic Server to log into a remote system on behalf of a subject that has already been authenticated. You must have one Credential Mapping provider in a security realm, and you can configure multiple Credential Mapping providers in a security realm.

[Customize this table](#)

**Credential Mapping Providers**

New Delete Reorder Showing 1 to 2 of 2 Previous Next

| <input type="checkbox"/> | Name                    | Description  | Version |
|--------------------------|-------------------------|--|---------|
| <input type="checkbox"/> | DefaultCredentialMapper | WebLogic Credential Mapping Provider   | 1.0     |
| <input type="checkbox"/> | MySAML2Provider         | WebLogic SAML Credential Mapping Provider. Supports Security Assertion Markup Language v1.1. | 2.0     |

New Delete Reorder Showing 1 to 2 of 2 Previous Next

8. Open the Provider Specific tab. The Provider Specific Settings Pane displays (see [Figure 14-93](#)).

**Figure 14–93 Provider Specific Settings Pane**

The screenshot shows the 'Settings for MySAML2Provider' configuration pane. It has three tabs: 'Configuration', 'Management', and 'Migration'. Under 'Configuration', there are two sub-tabs: 'Common' and 'Provider Specific'. The 'Provider Specific' tab is active. At the top left of the pane is a 'Save' button. Below it is a message: 'Use this page to configure provider-specific information for this SAML Credential Mapping Version 2 provider.' The main area contains several rows of configuration fields, each with a label, a text input field, and a description. The fields are: 'Issuer URI' (example.com/webcenter), 'Name Qualifier' (example.com), 'Default Time To Live' (120), 'Default Time To Live Offset' (0), 'Signing Key Alias' (testalias), 'Signing Key Pass Phrase' (masked with dots), 'Confirm Signing Key Pass Phrase' (masked with dots), and 'Default Name Mapper Class Name' (empty). Each field has a 'More Info...' link next to its description. At the bottom left of the pane is another 'Save' button.

- Configure the SAML Credential Mapping provider as a SAML authority, using the **Issuer URI**, **Name Qualifier**, and other attributes as shown below in [Table 14–3](#). Leave the remaining parameters set to their default values.

**Table 14–3 SAML Credential Mapping Provider Security Realm Settings**

| Parameter                               | Value                            | Description   |
|---|----------------------------------|---|
| Issuer URI                              | http://www.example.com/webcenter | The Issuer URI (name) of this SAML Authority. This unique URI tells the destination site (Wiki service) the origin of the SAML message and allows it to match with the key. Typically, the URI is used to guarantee uniqueness.   |
| Name Qualifier                          | example.com                      | The Name Qualifier value used by the Name Mapper. The value of the Name Qualifier is the security or administrative domain that qualifies the name of the subject. This provides a means to federate names from disparate user stores while avoiding the possibility of subject name collision. |
| Web Service Assertion Signing Key Alias |                                  | The alias used to retrieve from the keystore the key that is used to sign assertions (for example, testalias).  |

**Table 14–3 (Cont.) SAML Credential Mapping Provider Security Realm Settings**

| Parameter                                    | Value | Description   |
|--|-------|---|
| Web Service Assertion Signing Key Passphrase |       | The credential (password) used to retrieve from the keystore the keys used to sign assertions (for example, testkeypass). |
| Please type again To confirm                 |       | Re-enter the credential password.   |

10. Click **Save** to save your settings.

11. Restart the WebLogic Administration server.

#### 14.7.3.2.4 Configuring a Relying Party

Configuring a relying party is the second of two steps required to configure the credential mapping provider:

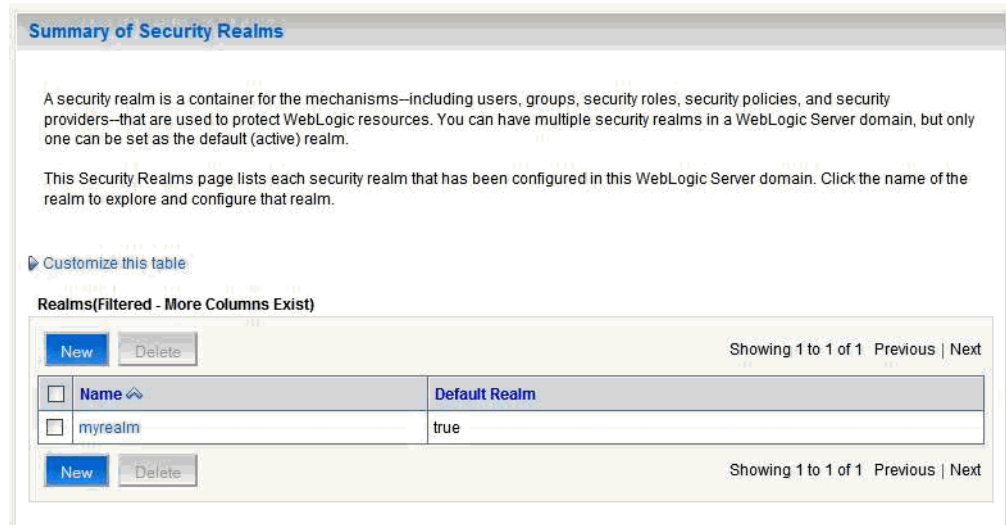
- Creating the SAML Credential Mapping Provider instance
- Configuring a relying party for each of the participating service applications (which can include OWC Wiki, OWC Discussions, RSS, Worklist Community Detail, Worklist SDP, and Worklist Integration)

To configure a relying party:

1. From the Domain Structure pane, click **Security Realms**.

The Summary of Security Realms pane displays (see [Figure 14–94](#)).

**Figure 14–94 Summary of Security Realms Pane**



2. Click your security realm and open the Providers tab and the Credential Mapping subtab.

The Credential Mapping Providers Settings pane displays (see [Figure 14–95](#)).

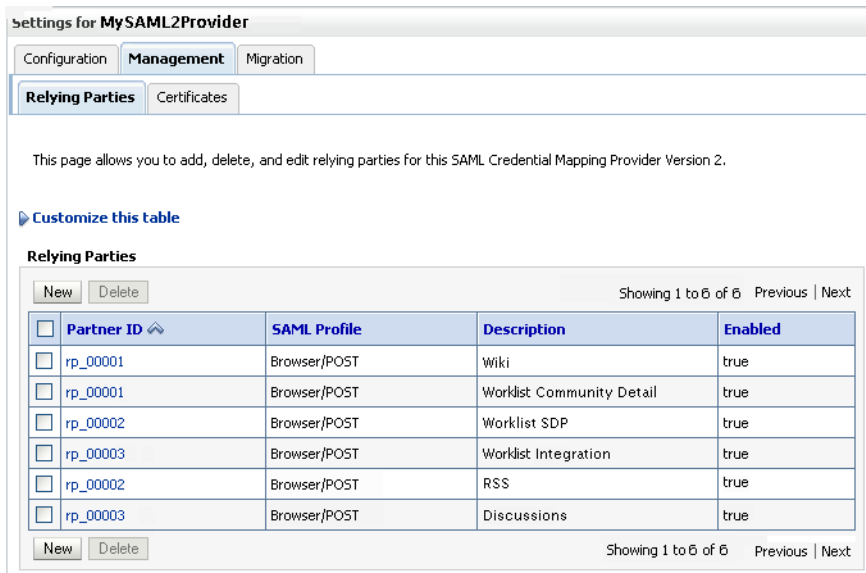
**Figure 14–95 Credential Mapping Providers Settings Pane**



3. Click the SAML Credential Mapping Provider you created.
4. Open the Management tab and the Relying Parties tab on the Settings page for the provider.

The Relying Parties Management Settings pane displays (see [Figure 14–96](#)).

**Figure 14–96 Relying Parties Management Settings Pane**



This screenshot shows the Relying Parties Management Settings pane.

\*\*\*\*\*

5. Click **New**.

The Create a New Relying Parties page displays (see [Figure 14–97](#)).

**Figure 14–97 Create a New Relying Party Page**

**Create a New Relying Party**

OK Cancel

**New Relying Party**

Please select a SAML profile to be used with your new Relying Party. You may enter a description if desired.

Please select a SAML Profile for the new SAML Relying Party.

**Profile:** Browser/POST

Please provide a description of the new SAML Relying Party.

**Description:**

OK Cancel

6. Select **Browser/POST** as the SAML **Profile**, and provide a **Description** (for example, *Wiki*).
7. Click **OK** to save your settings.
8. On the Relying Parties Management Settings pane, click the Partner ID of the Relying Party you just created (the Partner ID is automatically generated for you). The Relying Party Settings page displays (see [Figure 14–98](#)).

**Figure 14–98 Relying Party Settings Page**

**Settings for MySAML2Provider**

Specify the configuration of this Relying Party.

|  |  |  |
|--|--|--|
| <b>Partner ID:</b>                                 | rp_00001   | The ID of this SAML Relying Party. <a href="#">More Info...</a>                              |
| <b>Profile:</b>                                    | Browser/POST   | The SAML profile used by this SAML Relying Party. <a href="#">More Info...</a>               |
| <input checked="" type="checkbox"/> <b>Enabled</b> |  | The state of this SAML Relying Party. <a href="#">More Info...</a>                           |
| <b>Description:</b>                                | <input type="text" value="wiki"/>                    | A short description of this SAML Relying Party. <a href="#">More Info...</a>                 |
| <b>Target URL:</b>                                 | <input type="text" value="http://example.com:8890"/> | The destination site URL for which authentication is requested. <a href="#">More Info...</a> |

---

**Profile Configuration**

|                                |  |   |
|--------------------------------|--|---|
| <b>Assertion Consumer URL:</b> | <input type="text" value="http://example.com:8888"/> | The URL at which an Assertion Consumer Service for this SAML Relying Party can be reached. <a href="#">More Info...</a> |
|--------------------------------|--|---|

**Assertion Consumer Parameters:**

&PID=ap\_00001

One or more optional query parameters, in the form name=value, that will be added to the ACS URL when redirecting to the destination site. In the case of POST profile, these parameters will be included as form variables when using the default POST form. If a custom POST form is in use, the parameters will be made available as a Map of names and values, but the form may or may not be constructed to include the parameters in the POSTed data.. [More Info...](#)

|                   |                      |   |
|-------------------|----------------------|---|
| <b>POST Form:</b> | <input type="text"/> | The POST form used with this SAML Relying Party. <a href="#">More Info...</a> |
|-------------------|----------------------|---|

---

**Assertion Configuration**

|                                       |                                |   |
|---------------------------------------|--------------------------------|---|
| <b>Audience URI:</b>                  | <input type="text"/>           | An optional set of SAML Audience URIs. If set, an incoming assertion must contain at least one of the specified URIs in order to be considered valid. <a href="#">More Info...</a>  |
| <b>Name Mapper Class:</b>             | <input type="text"/>           | The name mapper class used for this SAML Relying Party. <a href="#">More Info...</a>  |
| <b>Assertion Time To Live:</b>        | <input type="text" value="0"/> | The time to live, in seconds, of assertions generated for this SAML Relying Party. <a href="#">More Info...</a>   |
| <b>Assertion Time To Live Offset:</b> | <input type="text" value="0"/> | A time factor you can use to allow the Credential Mapper to compensate for clock differences between the source and destination sites. The value is a positive or negative integer representing seconds. <a href="#">More Info...</a> |

- On the Relying Parties page, use the settings shown in [Table 14–4](#) to configure a relying party for the Wiki service. Leave the remaining parameters set to their default values. Click **Save** when finished.

**Table 14–4 Relying Party Settings for Wiki Service**

| Parameter   | Value    | Description   |
|-------------|----------|---|
| Enabled     | Checked  | The state of this SAML Relying Party.   |
| Description | OWC Wiki | A short description of this Relying Party   |
| Target URL  |          | The destination site URL for which authentication is requested (for example: <code>http://example.com:8890/owc_wiki/user/login.jz</code> ). |

**Table 14–4 (Cont.) Relying Party Settings for Wiki Service**

| Parameter                     | Value         | Description  |
|-------------------------------|---------------|--|
| Assertion Consumer URL        |               | <p>The URL at which an Assertion Consumer Service for this SAML Relying Party can be reached (for example, <code>http://example.com:8888/owc_wiki/samlacs/acs</code>).</p> <p>Indicates the URL to which an assertion or artifact should be POSTed or redirected.</p> <p><b>Note:</b> If you have checked <b>ACS requires SSL</b> while configuring destination site federation services, then use HTTPS protocol and the SSL port for the <code>WLS_Services</code> managed server.</p>                             |
| Assertion Consumer Properties | APID=ap_00001 | One or more optional query parameters, in the form <code>name=value</code> , that will be added to the ACS URL when redirecting to the destination site. In the case of POST profile, these parameters will be included as form variables when using the default POST form. In this case, <code>ap_00001</code> indicates the ID of the asserting party for the Wiki application configured in the SAML Identity Asserter of the WebCenter domain which provides the source site (WebCenter Spaces) and ITS details. |
| Sign Assertions               | Checked       | Specifies whether generated assertions for this SAML Relying Party are signed.   |
| Include KeyInfo               | Checked       | Indicates whether a <code>&lt;ds:keyinfo&gt;</code> element containing the signing certificate should be included when signing assertions. The default value is <code>true</code> . This value is ignored if <b>Sign Assertions</b> is false.  |

10. Repeat steps 1 - 8 to configure a relying party for the Worklist Community Detail service using the settings shown in [Table 14–5](#). Leave the remaining parameters on the Relying Parties page set to their default values. Click **Save** when finished.

**Table 14–5 Relying Party Settings for Worklist Community Detail**

| Parameter   | Value           | Description   |
|-------------|-----------------|---|
| Enabled     | Checked         | The state of this SAML Relying Party.   |
| Description | Worklist Detail | A short description of this Relying Party   |
| Target URL  |                 | <p>The destination site URL for which authentication is requested (for example: <code>http://example.com:8001/workflow/WebCenterWorklistDetail/faces/adf.task-flow</code>).</p> |

**Table 14–5 (Cont.) Relying Party Settings for Worklist Community Detail**

| Parameter                     | Value         | Description  |
|-------------------------------|---------------|--|
| Assertion Consumer URL        |               | The URL at which an Assertion Consumer Service for this SAML Relying Party can be reached (for example, <code>http://example.com:8888/workflow/WebCenterWorklistDetail/samlacs/acs</code> ).<br><br>Indicates the URL to which an assertion or artifact should be POSTed or redirected.<br><br><b>Note:</b> If you have checked <b>ACS requires SSL</b> while configuring destination site federation services, then use https protocol and the SSL port for the SOA managed server. |
| Assertion Consumer Properties | APID=ap_00001 | One or more optional query parameters, in the form name=value, that will be added to the ACS URL when redirecting to the destination site. In the case of POST profile, these parameters will be included as form variables when using the default POST form. In this case ap_00001 indicates the ID of the asserting party configured for Worklist Detail in the SAML Identity Asserter of the SOA domain, which provides the source site (WebCenter Spaces) and ITS details.       |
| Sign Assertions               | Checked       | Specifies whether generated assertions for this SAML Relying Party are signed.   |
| Include KeyInfo               | Checked       | Indicates whether a <ds:keyinfo> element containing the signing certificate should be included when signing assertions. The default value is true. This value is ignored if <b>Sign Assertions</b> is false.   |

- Repeat steps 1 - 8 to configure a relying party for the Worklist SDP service using the settings shown in [Table 14–6](#). Leave the remaining parameters on the Relying Parties pages set to their default values. Click **Save** when finished.

**Table 14–6 Relying Party Settings for Worklist SDP**

| Parameter   | Value         | Description   |
|-------------|---------------|---|
| Enabled     | Checked       | The state of this SAML Relying Party.   |
| Description | WebCenter SDP | A short description of this Relying Party   |
| Target URL  |               | The destination site URL for which authentication is requested (for example: <code>http://example.com:8001/workflow/sdpmessagingsca-ui-worklist/faces/adf.task-flow</code> ). |



**Table 14–6 (Cont.) Relying Party Settings for Worklist SDP**

| Parameter                     | Value         | Description  |
|-------------------------------|---------------|--|
| Assertion Consumer URL        |               | <p>The URL at which an Assertion Consumer Service for this SAML Relying Party can be reached (for example, <code>http://example.com:8888/workflow/sdp_messagingca-ui-worklist/samlacs/acs</code>).</p> <p>Indicates the URL to which an assertion or artifact should be POSTed or redirected.</p> <p><b>Note:</b> If you have checked <b>ACS requires SSL</b> while configuring destination site federation services, then use https protocol and the SSL port for the SOA managed server.</p>                               |
| Assertion Consumer Properties | APID=ap_00002 | <p>One or more optional query parameters, in the form <code>name=value</code>, that will be added to the ACS URL when redirecting to the destination site. In the case of POST profile, these parameters will be included as form variables when using the default POST form. In this case <code>ap_00002</code> indicates the ID of the asserting party configured for the Worklist SDP application in the SAML Identity Asserter of the SOA domain, which provides the source site (WebCenter Spaces) and ITS details.</p> |
| Sign Assertions               | Checked       | <p>Specifies whether generated assertions for this SAML Relying Party are signed.</p>  |
| Include KeyInfo               | Checked       | <p>Indicates whether a <code>&lt;ds:keyinfo&gt;</code> element containing the signing certificate should be included when signing assertions. The default value is <code>true</code>. This value is ignored if Sign Assertions is false.</p>   |

12. Repeat steps 1 - 8 to configure a relying party for the Worklist Integration service using the settings shown in [Table 14–7](#). Leave the remaining parameters on the Relying Parties pages set to their default values. Click **Save** when finished.

**Table 14–7 Relying Party Settings for Worklist Integration**

| Parameter   | Value         | Description  |
|-------------|---------------|--|
| Enabled     | Checked       | The state of this SAML Relying Party.  |
| Description | WebCenter SDP | A short description of this Relying Party  |
| Target URL  |               | <p>The destination site URL for which authentication is requested (for example: <code>http://example.com:8001/integration/worklistapp</code>).</p> |

**Table 14–7 (Cont.) Relying Party Settings for Worklist Integration**

| Parameter                     | Value         | Description  |
|-------------------------------|---------------|--|
| Assertion Consumer URL        |               | The URL at which an Assertion Consumer Service for this SAML Relying Party can be reached (for example, <code>http://example.com:8888/workflow/sdp/messaging-sca-ui-worklist/samlacs/acs</code> ).<br><br>Indicates the URL to which an assertion or artifact should be POSTed or redirected.<br><br><b>Note:</b> If you have checked <b>ACS requires SSL</b> while configuring destination site federation services, then use <code>https</code> protocol and the SSL port for the SOA managed server.                    |
| Assertion Consumer Properties | APID=ap_00003 | One or more optional query parameters, in the form <code>name=value</code> , that will be added to the ACS URL when redirecting to the destination site. In the case of POST profile, these parameters will be included as form variables when using the default POST form. In this case <code>ap_00003</code> indicates the ID of the asserting party configured for Worklist Integration application in the SAML Identity Asserter of the SOA domain, which provides the source site (WebCenter Spaces) and ITS details. |
| Sign Assertions               | Checked       | Specifies whether generated assertions for this SAML Relying Party are signed.   |
| Include KeyInfo               | Checked       | Indicates whether a <code>&lt;ds:keyinfo&gt;</code> element containing the signing certificate should be included when signing assertions. The default value is <code>true</code> . This value is ignored if <b>Sign Assertions</b> is false.  |

- Repeat steps 1 - 8 to configure a relying party for the RSS application using the settings shown in [Table 14–8](#). Leave the remaining parameters on the Relying Parties pages set to their default values. Click **Save** when finished.

**Table 14–8 Relying Party Settings for RSS**

| Parameter   | Value   | Description  |
|-------------|---------|--|
| Enabled     | Checked | The state of this SAML Relying Party.  |
| Description | RSS     | A short description of this Relying Party  |
| Target URL  |         | The destination site URL for which authentication is requested (for example: <code>http://example.com:8888/rss/rssserver</code> ). |

**Table 14–8 (Cont.) Relying Party Settings for RSS**

| Parameter                     | Value         | Description   |
|-------------------------------|---------------|---|
| Assertion Consumer URL        |               | <p>The URL at which an Assertion Consumer Service for this SAML Relying Party can be reached (for example, <code>http://example.com:8888/rss/samlacs/acs</code>).</p> <p>Indicates the URL to which an assertion or artifact should be POSTed or redirected.</p> <p><b>Note:</b> If you have checked <b>ACS requires SSL</b> while configuring destination site federation services, then use <code>https</code> protocol and the SSL port for the <code>WLS_Spaces</code> managed server.</p>            |
| Assertion Consumer Properties | APID=ap_00002 | <p>One or more optional query parameters, in the form <code>name=value</code>, that will be added to the ACS URL when redirecting to the destination site. In the case of POST profile, these parameters will be included as form variables when using the default POST form. In this case <code>ap_00002</code> indicates the ID of the asserting party configured for RSS in the SAML Identity Asserter of the WebCenter domain, which provides the source site (WebCenter Spaces) and ITS details.</p> |
| Sign Assertions               | Checked       | <p>Specifies whether generated assertions for this SAML Relying Party are signed.</p>   |
| Include KeyInfo               | Checked       | <p>Indicates whether a <code>&lt;ds:keyinfo&gt;</code> element containing the signing certificate should be included when signing assertions. The default value is <code>true</code>. This value is ignored if <b>Sign Assertions</b> is false.</p>   |

- Repeat steps 1 - 8 to configure a relying party for the Discussions application using the settings shown in [Table 14–9](#). Leave the remaining parameters on the Relying Parties pages set to their default values. Click **Save** when finished.

**Table 14–9 Relying Party Settings for Discussions**

| Parameter              | Value       | Description  |
|------------------------|-------------|--|
| Enabled                | Checked     | The state of this SAML Relying Party.  |
| Description            | Discussions | A short description of this Relying Party  |
| Target URL             |             | <p>The destination site URL for which authentication is requested (for example: <code>http://example.com:8890/owc_discussions/admin/content-main.jsp</code>).</p>  |
| Assertion Consumer URL |             | <p>The URL at which an Assertion Consumer Service for this SAML Relying Party can be reached (for example, <code>http://example.com:8890/owc_discussions/samlacs/acs</code>).</p> <p>Indicates the URL to which an assertion or artifact should be POSTed or redirected.</p> <p><b>Note:</b> If you have checked <b>ACS requires SSL</b> while configuring destination site federation services, then use <code>https</code> protocol and the SSL port for the managed server.</p> |

**Table 14–9 (Cont.) Relying Party Settings for Discussions**

| Parameter                     | Value         | Description  |
|-------------------------------|---------------|--|
| Assertion Consumer Properties | APID=ap_00003 | One or more optional query parameters, in the form name=value, that will be added to the ACS URL when redirecting to the destination site. In the case of POST profile, these parameters will be included as form variables when using the default POST form. In this case ap_00003 indicates the ID of the asserting party configured for the Discussions application in the SAML Identity Asserter of the WebCenter domain, which provides the source site (WebCenter Spaces) and ITS details. |
| Sign Assertions               | Checked       | Specifies whether generated assertions for this SAML Relying Party are signed.   |
| Include KeyInfo               | Checked       | Indicates whether a <ds:keyinfo> element containing the signing certificate should be included when signing assertions. The default value is true. This value is ignored if <b>Sign Assertions</b> is false.   |

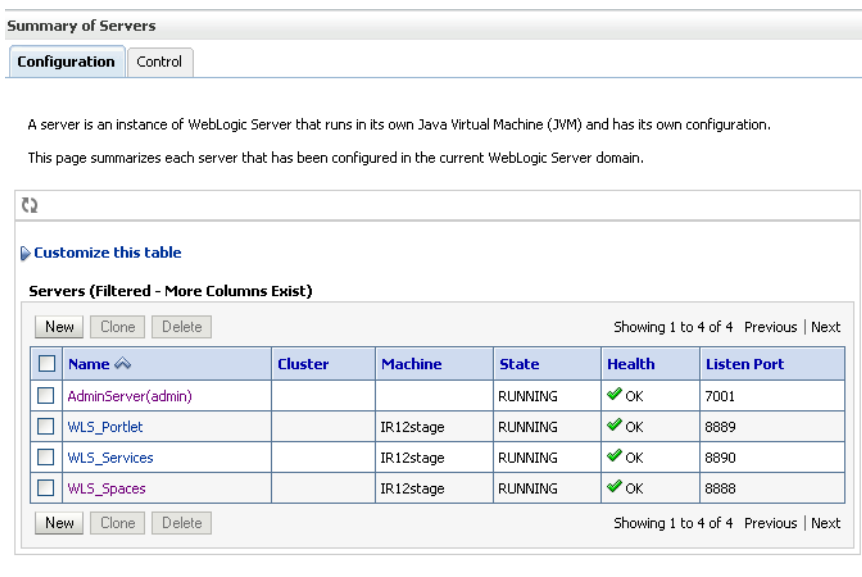
**14.7.3.2.5 Configuring Source Site Federation Services**

This section describes how to create and configure source site Federation services.

To configure Source Site Federation Services:

1. Log in to the WLS Administration Console.  
 For information on logging into the WLS Administration Console, see [Section 1.12.2, "Oracle WebLogic Server Administration Console"](#).
2. On the Domain Structure pane, expand the **Environment** node and click **Servers**.  
 The Summary of Servers page displays (see [Figure 14–99](#)).

**Figure 14–99 Summary of Servers Page**



3. Click **WLS\_Spaces** and open the Configuration tab.

4. Open the Federation Services subtab and the SAML 1.1 Source Site subtab.

The Federation Services Configuration SAML 1.1 Source Site Settings page for the WLS\_Spaces server displays (see [Figure 14–100](#)).

**Figure 14–100 Federation Services Configuration SAML 1.1 Source Site Settings Page**

**Settings for WLS\_Spaces**

Configuration Protocols Logging Debug Monitoring Control Deployments Services Security Notes

General Cluster Services Keystores SSL **Federation Services** Deployment Migration Tuning Overload

Health Monitoring Server Start

SAML 1.1 Source Site SAML 1.1 Destination Site SAML 2.0 General SAML 2.0 Identity Provider

SAML 2.0 Service Provider

Save

This page lets you view and define various Federation Services SAML 1.1 SSO Source Site settings for this server instance. You must first configure a SAML Credential Mapper V2 security provider in the server's security realm.

**Source Site Enabled** Indicates whether the Source Site is enabled. [More Info...](#)

**Source Site URL:**  The URL for the Source Site. [More Info...](#)

**Source Site ID Hex:**  The Source Site ID in hexadecimal. [More Info...](#)

**Source Site ID Base64:**  The Source Site ID base64-encoded. [More Info...](#)

**Signing Key Alias:**  The alias used to store and retrieve the Source Site's signing key in the keystore. This key is used to sign POST profile responses. [More Info...](#)

**Signing Key Passphrase:**  The passphrase used to retrieve the Source Site's signing key from the keystore. [More Info...](#)

**Confirm Signing Key Passphrase:**

**Intersite Transfer URIs:**  The Intersite Transfer URIs. [More Info...](#)

**ITS Requires SSL** Specifies whether the Intersite Transfer Service requires SSL. [More Info...](#)

**Assertion Retrieval URIs:**  One or more URIs on which to listen for incoming assertion retrieval requests. [More Info...](#)

5. Configure the SAML source site attributes as shown in [Figure 14–10](#). Leave the remaining parameters set to their default values.

**Table 14–10 Source Site Federation Services Parameters**

| Parameter           | Value   | Description   |
|---------------------|---------|---|
| Source Site Enabled | Checked | Allow the WebLogic server instance to serve as a SAML source site by setting Source Site Enabled to true. |

**Table 14–10 (Cont.) Source Site Federation Services Parameters**

| Parameter                | Value  | Description  |
|--------------------------|--|--|
| Source Site URL          |  | Set the URL for the SAML source site (for example, <code>http://example.com:8888/webcenter</code> ). This is the URL that hosts the Intersite Transfer Service and Assertion Retrieval Service. The source site URL is encoded as a source ID in hex and Base64.   |
| Signing Key Alias        |  | The SAML source site requires a trusted certificate with which to sign assertions. Add this certificate to the keystore and enter the alias (for example, <code>testalias</code> ) to be used to access the certificate. The server's SSL identity key/certificates will be used by default if a signing alias and passphrase are not supplied.        |
| Signing Key Passphrase   |  | The SAML source site requires a trusted certificate with which to sign assertions. Add this certificate to the keystore and enter the passphrase (for example, <code>testkeypass</code> ) to be used to access the certificate. The server's SSL identity key/certificates will be used by default if a signing alias and passphrase are not supplied. |
| Intersite Transfer URIs  | <code>/webcenter/samlits/its</code> [add on top, leave the rest] | Specify the URIs for the Intersite Transfer Service. These URIs are also specified in the configuration of an Asserting Party.   |
| Assertion Retrieval URIs | <code>/webcenter/samlars/ars</code> [add on top, leave the rest] | N/A - URI for Assertion Retrieval Service used when artifact profile is used.  |
| ITS Requires SSL         | Unchecked  | <b>Note:</b> If you check this, then you need to change the Source Site ITS URL specified in the SAML Asserting Party configuration in the SAML Identity provider as HTTPS and the server's SSL port.  |
| ARS Requires SSL         | Unchecked  | Applicable only when Artifact profile is used  |

6. Click **Save** to save your settings when done.
7. Restart the `WLS_Spaces` managed server.

#### 14.7.3.2.6 Configuring the SAML Identity Assertion Provider

This section describes how to create and configure a SAML Identity Assertion Provider V2 instance (the SAML Identity Assertion provider is not part of the default security realm). This section also describes how to establish trust by registering the source site's SSL certificate in the certificate registry maintained by the SAML Identity Assertion provider.

#### To create a SAML Identity Assertion Provider

1. Log in to the WLS Administration Console.
 

For information on logging into the WLS Administration Console, see [Section 1.12.2, "Oracle WebLogic Server Administration Console"](#).
2. From the Domain Structure pane, click **Security Realms**.
 

The Summary of Security Realms pane displays (see [Figure 14–101](#)).

**Figure 14–101 Summary of Security Realms Pane**

**Summary of Security Realms**

A security realm is a container for the mechanisms—including users, groups, security roles, security policies, and security providers—that are used to protect WebLogic resources. You can have multiple security realms in a WebLogic Server domain, but only one can be set as the default (active) realm.

This Security Realms page lists each security realm that has been configured in this WebLogic Server domain. Click the name of the realm to explore and configure that realm.

[Customize this table](#)

**Realms(Filtered - More Columns Exist)**

New Delete Showing 1 to 1 of 1 Previous | Next

| <input type="checkbox"/> | Name ↕  | Default Realm |
|--------------------------|---------|---------------|
| <input type="checkbox"/> | myrealm | true          |

New Delete Showing 1 to 1 of 1 Previous | Next

3. Click your security realm.

The Settings page for the security realm displays (see [Figure 14–102](#)).

**Figure 14–102 Security Realm Settings Page**

**Settings for myrealm**

Configuration **Users and Groups** Roles and Policies Credential Mappings Providers Migration

General **RDBMS Security Store** User Lockout Performance

Save

Use this page to configure the general behavior of this security realm.

Note:  
If you are implementing security using JACC (Java Authorization Contract for Containers as defined in JSR 115), you must use the DD Only security model. Other WebLogic Server models are not available and the security functions for Web applications and EJBs in the Administration Console are disabled.

**Name:** myrealm The name of this security realm. [More Info...](#)

**Security Model Default:** DD Only Specifies the default security model for Web applications or EJBs that are secured by this security realm. You can override this default during deployment. [More Info...](#)

**Combined Role Mapping Enabled** Determines how the role mappings in the Enterprise Application, Web application, and EJB containers interact. This setting is valid only for Web applications and EJBs that use the Advanced security model and that initialize roles from deployment descriptors. [More Info...](#)

**Use Authorization Providers to Protect JMX Access** Configures the WebLogic Server MBean servers to use the security realm's Authorization providers to determine whether a JMX client has permission to access an MBean attribute or invoke an MBean operation. [More Info...](#)

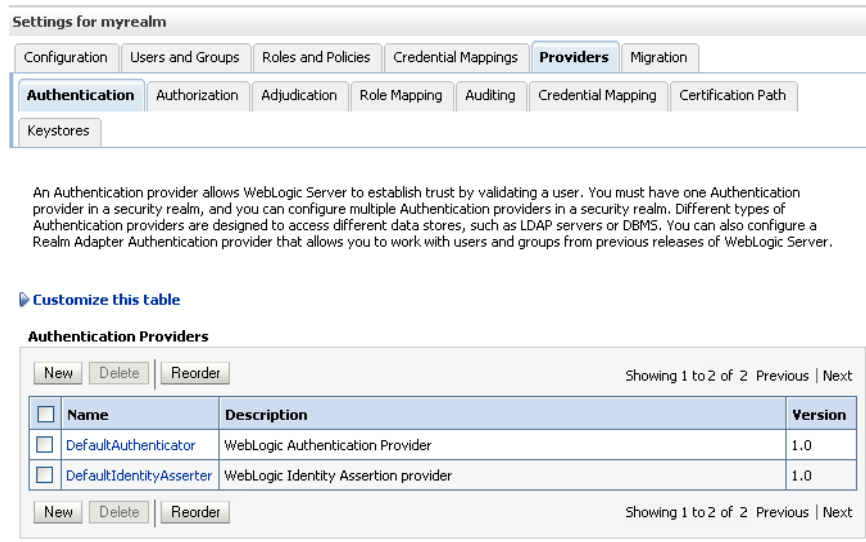
Advanced

Save

4. Open the Providers tab and select the Authentication subtab.

The Authentication Settings pane displays (see [Figure 14–103](#)).

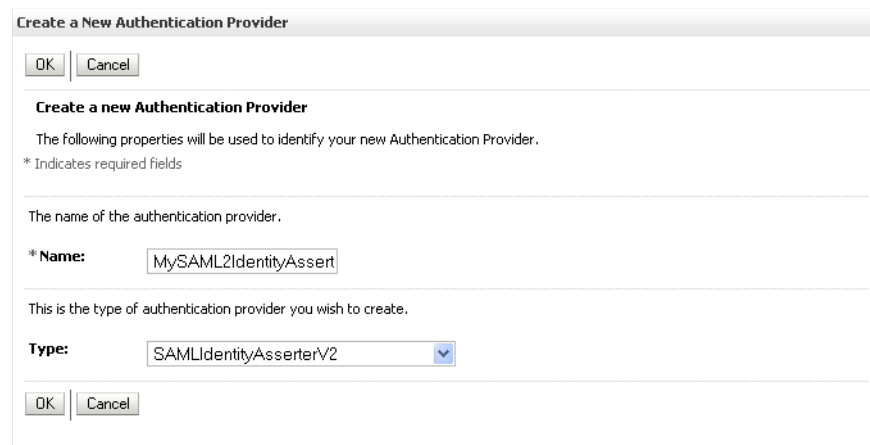
**Figure 14–103 Authentication Settings Pane**



5. Click **New**.

The Create a New Authentication Provider page displays (see [Figure 14–104](#)).

**Figure 14–104 Create a New Authentication Provider Page**



6. Enter a **Name** for the new SAML Identity Asserter, and select the **Type** as SAMLIdentityAsserterV2.
7. Click **OK** to save your settings.
8. Restart the WebLogic Administration server if indicated in the Messages area.
9. Go to the SOA domain and create a SAML Identity Asserter provider there as well using the steps above.

**To configure a certificate for the SAML ID Asserter**

1. Log in to the WLS Administration Console.



For information on logging into the WLS Administration Console, see [Section 1.12.2, "Oracle WebLogic Server Administration Console"](#).

2. From the Domain Structure pane, click **Security Realms**.

The Summary of Security Realms pane displays (see [Figure 14–105](#)).

**Figure 14–105 Summary of Security Realms Pane**

**Summary of Security Realms**

A security realm is a container for the mechanisms—including users, groups, security roles, security policies, and security providers—that are used to protect WebLogic resources. You can have multiple security realms in a WebLogic Server domain, but only one can be set as the default (active) realm.

This Security Realms page lists each security realm that has been configured in this WebLogic Server domain. Click the name of the realm to explore and configure that realm.

[Customize this table](#)

**Realms(Filtered - More Columns Exist)**

New Delete Showing 1 to 1 of 1 Previous | Next

| <input type="checkbox"/> | Name ↕  | Default Realm |
|--------------------------|---------|---------------|
| <input type="checkbox"/> | myrealm | true          |

New Delete Showing 1 to 1 of 1 Previous | Next

3. Click your security realm.

The Settings page for the security realm displays (see [Figure 14–106](#)).

**Figure 14–106 Security Realm Settings Page**

**Settings for myrealm**

Configuration **Users and Groups** Roles and Policies Credential Mappings Providers Migration

General **RDBMS Security Store** User Lockout Performance

Save

Use this page to configure the general behavior of this security realm.

Note:  
If you are implementing security using JACC (Java Authorization Contract for Containers as defined in JSR 115), you must use the DD Only security model. Other WebLogic Server models are not available and the security functions for Web applications and EJBs in the Administration Console are disabled.

**Name:** myrealm The name of this security realm. [More Info...](#)

**Security Model Default:** DD Only Specifies the default security model for Web applications or EJBs that are secured by this security realm. You can override this default during deployment. [More Info...](#)

**Combined Role Mapping Enabled** Determines how the role mappings in the Enterprise Application, Web application, and EJB containers interact. This setting is valid only for Web applications and EJBs that use the Advanced security model and that initialize roles from deployment descriptors. [More Info...](#)

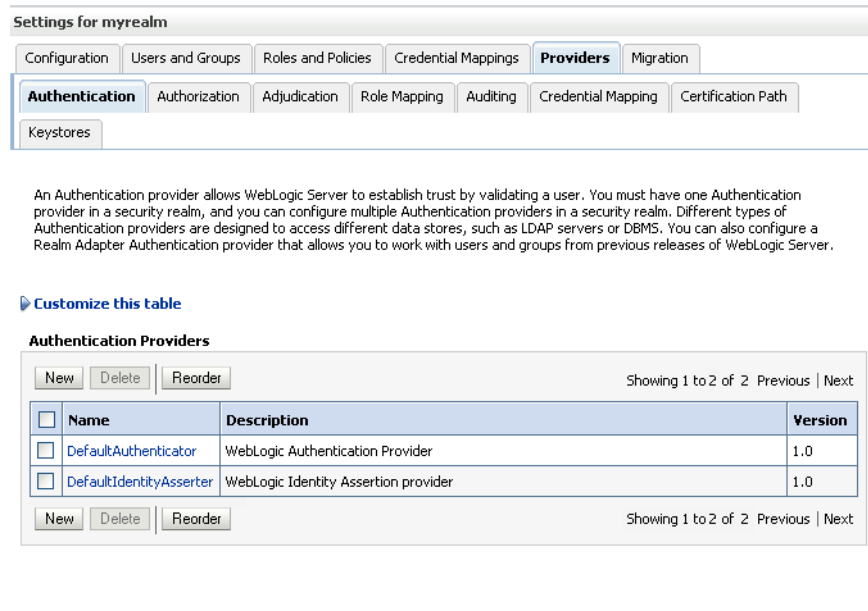
**Use Authorization Providers to Protect JMX Access** Configures the WebLogic Server MBean servers to use the security realm's Authorization providers to determine whether a JMX client has permission to access an MBean attribute or invoke an MBean operation. [More Info...](#)

Advanced

Save

4. Open the Providers tab and select the Authentication subtab.  
The Authentication Settings pane displays (see [Figure 14–107](#)).

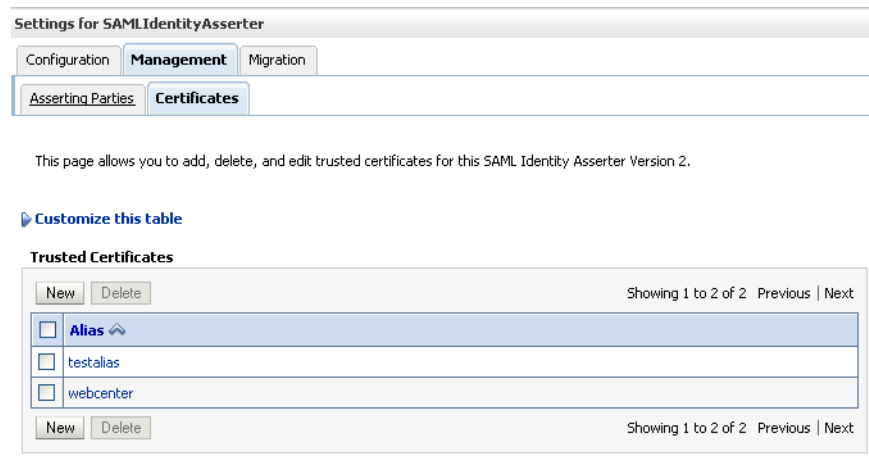
**Figure 14–107 Authentication Settings Pane**



5. Click the SAML Identity Asserter you created and open the Management tab and the Certificates subtab.

The Certificate Settings pane displays (see [Figure 14–108](#)).

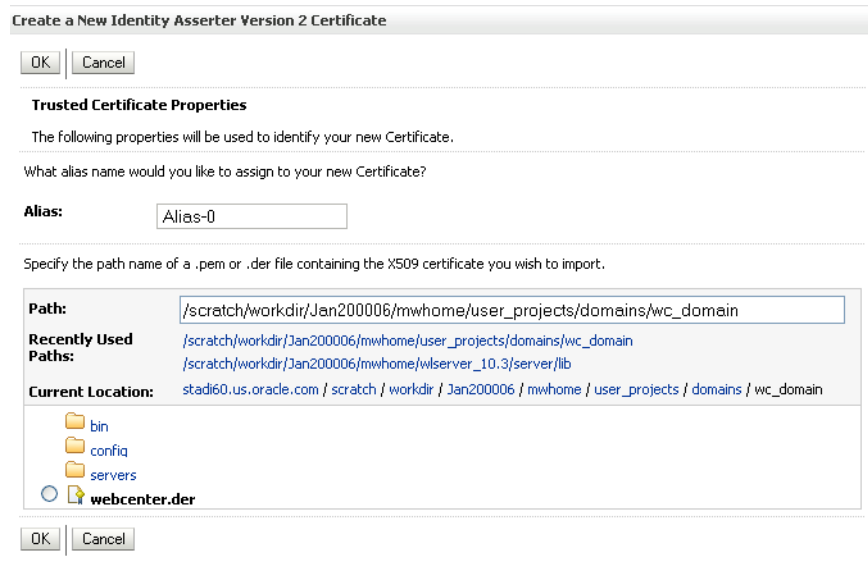
**Figure 14–108 Certificate Settings Pane**



6. Click **New**.

The Create a New Identity Asserter Certificate page displays (see [Figure 14–109](#)).

**Figure 14–109 Create a New Identity Asserter Certificate Page**



7. Configure the certificate as shown in [Table 14–11](#).

**Table 14–11 Certificates Page Parameters**

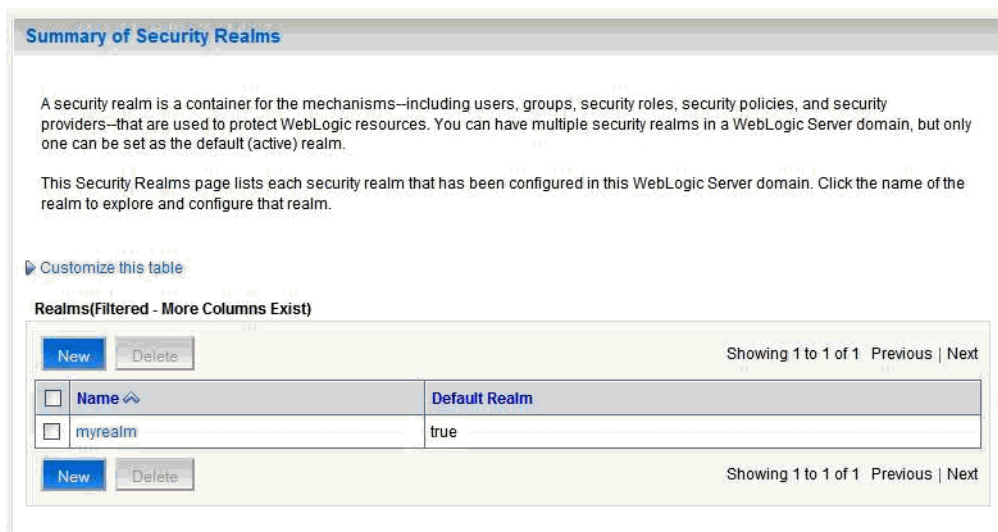
| Parameter | Value | Description  |
|-----------|-------|--|
| alias     |       | The name to assign to your new Certificate This is the alias of the keystore you created in <a href="#">Section 14.7.3.2.2, "Generating and Registering Certificates"</a> .                                |
| Path      |       | Specify the path name of the .der file containing the X509 certificate you wish to import. This is the file you created in <a href="#">Section 14.7.3.2.2, "Generating and Registering Certificates"</a> . |

8. Click **OK** to save your settings.
9. Repeat the previous step for the SAML ID Asserter created in the SOA domain. Be sure to copy over `testalias.der` (assuming that this was the name given to your .DER file) from your WebLogic Home to the machine hosting the SOA domain.

**To Configure an Asserting Party**

1. Log in to the WLS Administration Console.  
For information on logging into the WLS Administration Console, see [Section 1.12.2, "Oracle WebLogic Server Administration Console"](#).
2. From the Domain Structure pane, click **Security Realms**.  
The Summary of Security Realms pane displays (see [Figure 14–110](#)).

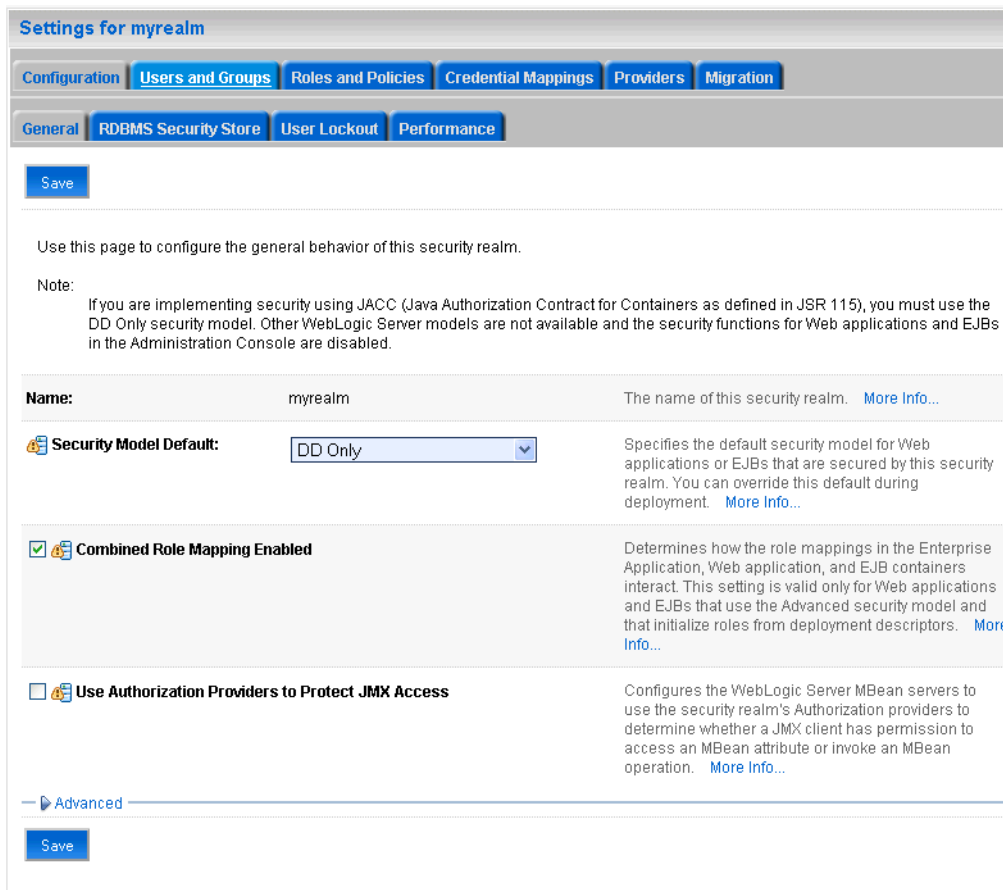
Figure 14–110 Summary of Security Realms Pane



3. Click your security realm.

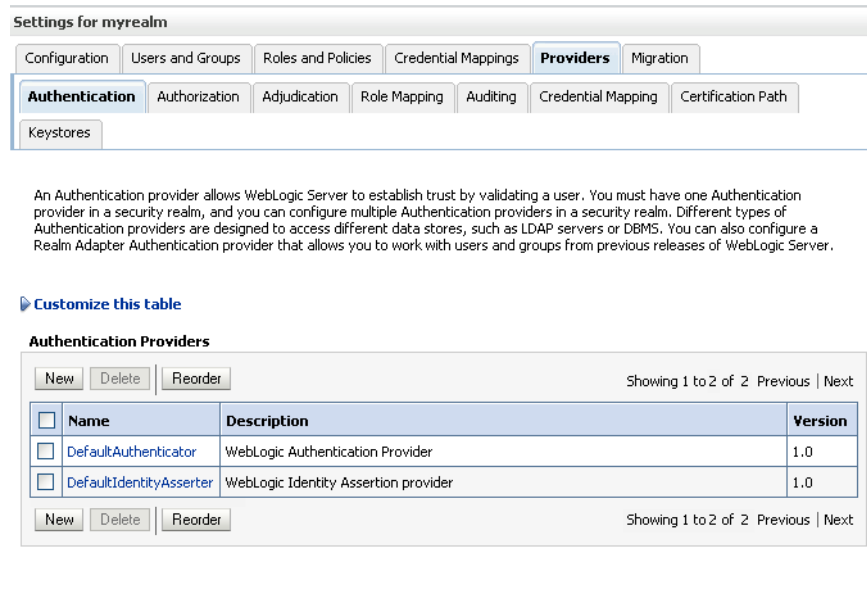
The Settings page for the security realm displays (see Figure 14–111).

Figure 14–111 Security Realm Settings Page



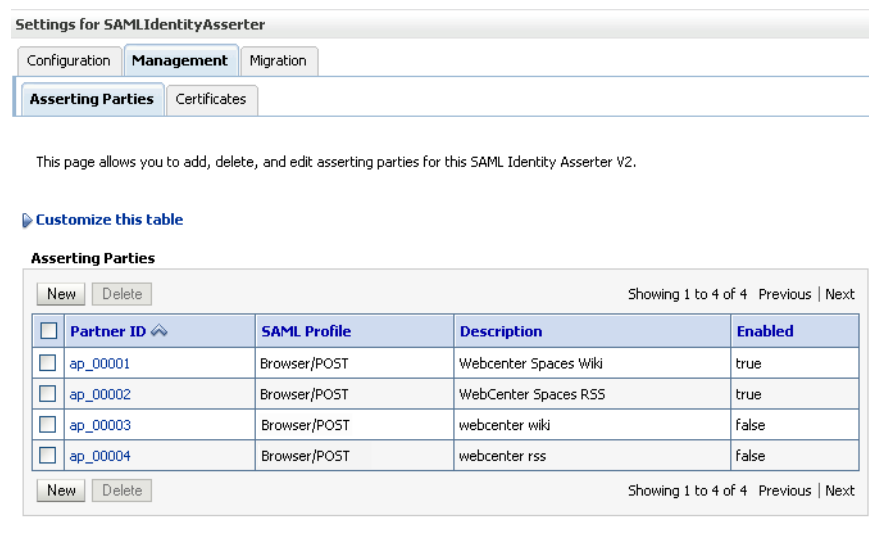
- Open the Providers tab and select the Authentication subtab.  
The Authentication Settings pane displays (see [Figure 14–112](#)).

**Figure 14–112 Authentication Settings Pane**



- Click the SAML Identity Asserter you created and open the Management tab and the Asserting Parties subtab.  
The Asserting Parties Settings pane displays (see [Figure 14–113](#)).

**Figure 14–113 Asserting Parties Settings Pane**



- Click **New**.  
The Create a New Asserting Party page displays (see [Figure 14–114](#)).

**Figure 14–114 Create a New Asserting Party Page**

**Create a New Asserting Party**

OK Cancel

**New Asserting Party**

Please select a SAML profile to be used with your new Asserting Party. You may enter a description if desired.

Please select a SAML Profile for the new SAML Asserting Party.

**Profile:** Browser/POST

Please provide a description of the new SAML Asserting Party.

**Description:**

OK Cancel

7. Select the **Profile** and provide a **Description** for the Asserting Party.  
Use the same SAML profile you chose for the corresponding relying party (for example, Browser / POST).
8. Click **OK** to save your settings.
9. From the Asserting Parties Settings pane, click the Partner ID of the Asserting Party you just created (the Partner ID is assigned automatically).  
The Settings page for the new Asserting Party displays (see [Figure 14–115](#)).

**Figure 14–115 Asserting Party Settings Page**

**Settings for SAMLIdentityAsserter**

Configure an Asserting Party that can generate SAML assertions consumed by this SAML Identity Assertion provider.

|  |   |  |
|--|---|--|
| <b>Partner ID:</b>                                 | ap_00001  | The Asserting Party ID. <a href="#">More Info...</a>   |
| <b>Profile:</b>                                    | Browser/POST                                      | The SAML profile used with this partner: one of Browser/Artifact, Browser/POST, WSS/Sender-Vouches, or WSS/Holder-of-Key. <a href="#">More Info...</a> |
| <input checked="" type="checkbox"/> <b>Enabled</b> |   | Specifies whether this Asserting Party can be used to obtain SAML assertions. <a href="#">More Info...</a>   |
| <b>Description:</b>                                | <input type="text" value="Webcenter Spaces Wik"/> | A short description of this Asserting Party. <a href="#">More Info...</a>  |
| <b>Target URL:</b>                                 | <input type="text" value="http://example.com"/>   | The target URL of this SAML Asserting Party. <a href="#">More Info...</a>  |

**Profile Configuration**

|  |  |  |
|--|--|--|
| <b>POST Signing Certificate Alias:</b> | <input type="text" value="webcenter"/>               | The alias of the certificate trusted for verifying signatures on SAML protocol elements from this Asserting Party. Must be set for Browser/POST profile. <a href="#">More Info...</a>  |
| <b>Source Site Redirect URIs:</b>      | <input type="text" value="/owc_wiki/user/login.jz"/> | An optional set of URIs from which unauthenticated users will be redirected to the configured ITS URL. If set, the IntersiteTransferURL must also be set. <a href="#">More Info...</a> |
| <b>Source Site ITS URL:</b>            | <input type="text" value="http://example.com"/>      | The Intersite Transfer Service (ITS) URL of the SAML Source Site for this Asserting Party. <a href="#">More Info...</a>  |
| <b>Source Site ITS Parameters:</b>     | <input type="text" value="RPID=rp_00001"/>           | Optionally, zero or more query parameters, of the form name=value, that will be added to the ITS URL when redirecting to the source site. <a href="#">More Info...</a>                 |

- Configure the Asserting Party for the WC domain Wiki service as shown in [Table 14–12](#). For more information, see [Table 14–4, "Relying Party Settings for Wiki Service"](#).

**Table 14–12 WC Domain - Asserting Party for Wiki**

| Parameter                      | Value   | Description  |
|--------------------------------|---------|--|
| Enabled                        | Checked | Specifies whether this Asserting Party can be used to obtain SAML assertions   |
| Description                    |         | A short description of this Asserting Party (for example, WebCenter Spaces for Wiki)   |
| Target URL                     |         | The target URL of this SAML Asserting Party (for example, <code>http://example.com:8888/webcenter</code> )   |
| POST Signing Certificate alias |         | The alias of the certificate trusted for verifying signatures on SAML protocol elements from this Asserting Party (for example, <code>testalias</code> ). Must be set when using the Browser/POST profile. |



**Table 14–12 (Cont.) WC Domain - Asserting Party for Wiki**

| Parameter                           | Value                   | Description  |
|-------------------------------------|-------------------------|--|
| Source Site Redirect URIs           | /owc_wiki/user/login.jz | An optional set of URIs from which unauthenticated users will be redirected to the configured ITS URL. If set, the IntersiteTransferURL must also be set.<br><br><b>Note:</b> Based on this setting, when you first access the destination site, you are redirected to the configured ITS URL (which in this case is within the source application), your session is established with the source application and then redirected to the destination site.  |
| Source Site ITS URL                 |                         | The Intersite Transfer Service (ITS) URL of the SAML Source Site for this Asserting Party (for example, <a href="http://example.com:8888/webcenter/samlits/its">http://example.com:8888/webcenter/samlits/its</a> ).<br><br>Used with SSO profiles only, to support the destination site first scenario, whereby a user tries to access a destination site URL prior to being authenticated and is redirected to the source site to be authenticated and obtain a SAML assertion. The Redirect URIs attribute must also be configured for source-site redirection to work.<br><br><b>Note:</b> If you check <b>ITS requires SSL</b> in Source Site Federation Services, you must also change the Source Site ITS URL to use HTTPS and the server's SSL port. |
| Source Site ITS parameters          | RPID=rp_00001           | Optionally, zero or more query parameters, of the form name=value, that will be added to the ITS URL when redirecting to the source site. In this case, rp_00001 is the relying party ID for the OWC Wiki application specified in the SAML Credential Mapping Provider of the WebCenter domain which provides the destination site details. For more information, see <a href="#">Table 14–4, "Relying Party Settings for Wiki Service"</a> .   |
| Issuer URI                          |                         | The issuer URI of the SAML Authority issuing assertions for this SAML Asserting Party (for example, <a href="http://www.example.com/webcenter">http://www.example.com/webcenter</a> ).   |
| Signature Required                  | Checked                 | If true, assertions must be signed. If false, signature elements are not required, but will be verified if present.  |
| Assertion Signing Certificate alias |                         | The alias of the certificate trusted for verifying signatures on assertions from this Asserting Party (for example, testalias). This must be set if <b>Signature Required</b> is checked. The certificate must also be registered in the SAML Identity Asserter's certificate registry.  |

11. Click **Save** to save your settings.
12. Repeat steps 1 - 11 using the settings shown in [Table 14–13](#) to configure the Asserting party for the WC domain RSS application.

**Table 14–13 WC Domain - Asserting Party for RSS**

| Parameter                      | Value                        | Description   |
|--------------------------------|------------------------------|---|
| Enabled                        | Checked                      | Specifies whether this Asserting Party can be used to obtain SAML assertions.   |
| Description                    |                              | A short description of this Asserting Party (for example, <i>WebCenter Spaces for RSS</i> )   |
| Target URL                     |                              | The target URL of this SAML Asserting Party (for example, <code>http://example.com:8888/webcenter</code> )  |
| POST Signing Certificate alias |                              | The alias of the certificate trusted for verifying signatures on SAML protocol elements from this Asserting Party (for example, <code>testalias</code> ). Must be set when using the Browser/POST profile.  |
| Source Site Redirect URIs      | <code>/rss/rssservlet</code> | An optional set of URIs from which unauthenticated users will be redirected to the configured ITS URL. If set, the <code>IntersiteTransferURL</code> must also be set.<br><br><b>Note:</b> Based on this setting, when you first access the destination site, you are redirected to the configured ITS URL (which in this case is within the source application), your session is established with the source application and then redirected to the destination site.  |
| Source Site ITS URL            |                              | The Intersite Transfer Service (ITS) URL of the SAML Source Site for this Asserting Party (for example, <code>http://example.com:8888/webcenter/samlits/its</code> ).<br><br>Used with SSO profiles only, to support the destination site first scenario, whereby a user tries to access a destination site URL prior to being authenticated and is redirected to the source site to be authenticated and obtain a SAML assertion. The Redirect URIs attribute must also be configured for source-site redirection to work.<br><br><b>Note:</b> If you check <b>ITS requires SSL</b> in Source Site Federation Services, you must also change the Source Site ITS URL to use HTTPS and the server's SSL port. |
| Source Site ITS parameters     | <code>RPID=rp_00002</code>   | Optionally, zero or more query parameters, of the form <code>name=value</code> , that will be added to the ITS URL when redirecting to the source site. In this case <code>rp_00005</code> is the relying party ID for RSS specified in the SAML Credential Mapping provider of the WebCenter domain which provides the destination site details. See <a href="#">Table 14–8, "Relying Party Settings for RSS"</a> for more information about RSS settings.   |
| Issuer URI                     |                              | The issuer URI of the SAML Authority issuing assertions for this SAML Asserting Party (for example, <code>http://www.example.com/webcenter</code> ).  |
| Signature Required             | Checked                      | If true, assertions must be signed. If false, signature elements are not required, but will be verified if present.   |

**Table 14–13 (Cont.) WC Domain - Asserting Party for RSS**

| Parameter                           | Value | Description   |
|-------------------------------------|-------|---|
| Assertion Signing Certificate alias |       | The alias of the certificate trusted for verifying signatures on assertions from this Asserting Party (for example, <code>testalias</code> ). This must be set if <b>Signature Required</b> is checked. The certificate must also be registered in the SAML Identity Asserter's certificate registry. |

13. Repeat steps 1 - 11 using the settings shown in [Table 14–14](#) to configure the Asserting party for the WC domain Discussions application.

**Table 14–14 WC Domain - Asserting Party for RSS**

| Parameter                      | Value   | Description   |
|--------------------------------|---|---|
| Enabled                        | Checked   | Specifies whether this Asserting Party can be used to obtain SAML assertions.   |
| Description                    |   | A short description of this Asserting Party (for example, <code>WebCenter Spaces for Discussions</code> )   |
| Target URL                     |   | The target URL of this SAML Asserting Party (for example, <code>http://example.com:8888/webcenter</code> )  |
| POST Signing Certificate alias |   | The alias of the certificate trusted for verifying signatures on SAML protocol elements from this Asserting Party (for example, <code>testalias</code> ). This must be set when using the Browser/POST profile.   |
| Source Site Redirect URIs      | <code>/owc_discussions/admin/content-main.jsp</code><br><code>/owc_discussions/login!withRedirect.jspa</code><br><code>/owc_discussions/login!default.jspa</code><br><code>/owc_discussions/login.jspa</code> | <p>An optional set of URIs from which unauthenticated users will be redirected to the configured ITS URL. If set, the <code>IntersiteTransferURL</code> must also be set.</p> <p><b>Note:</b> Based on this setting, when you first access the destination site, you are redirected to the configured ITS URL (which in this case is within the source application), your session is established with the source application and then redirected to the destination site.</p> |

**Table 14–14 (Cont.) WC Domain - Asserting Party for RSS**

| Parameter                           | Value         | Description   |
|-------------------------------------|---------------|---|
| Source Site ITS URL                 |               | <p>The Intersite Transfer Service (ITS) URL of the SAML Source Site for this Asserting Party (for example, <code>http://example.com:8888/webcenter/samlits/its</code>).</p> <p>Used with SSO profiles only, to support the destination site first scenario, whereby a user tries to access a destination site URL prior to being authenticated and is redirected to the source site to be authenticated and obtain a SAML assertion. The Redirect URIs attribute must also be configured for source-site redirection to work.</p> <p><b>Note:</b> If you check <b>ITS requires SSL</b> in Source Site Federation Services, you must also change the Source Site ITS URL to use HTTPS and the server's SSL port.</p> |
| Source Site ITS parameters          | RPID=rp_00006 | <p>Optionally, zero or more query parameters, of the form name=value, that will be added to the ITS URL when redirecting to the source site. In this case <code>rp_00006</code> is the relying party ID for OWC Discussions specified in the SAML Credential Mapping provider of the WebCenter domain which provides the destination site details. See <a href="#">Table 14–8, "Relying Party Settings for RSS"</a> for more information about RSS settings.</p>  |
| Issuer URI                          |               | <p>The issuer URI of the SAML Authority issuing assertions for this SAML Asserting Party (for example, <code>http://www.example.com/webcenter</code>).</p>  |
| Signature Required                  | Checked       | <p>If true, assertions must be signed. If false, signature elements are not required, but will be verified if present.</p>  |
| Assertion Signing Certificate alias |               | <p>The alias of the certificate trusted for verifying signatures on assertions from this Asserting Party (for example, <code>testalias</code>). This must be set if <b>Signature Required</b> is checked. The certificate must also be registered in the SAML Identity Asserter's certificate registry.</p>   |

- Change domains to the SOA domain and repeat steps 1 - 11 using the settings shown in [Table 14–15](#) to configure the Asserting Party for the SOA domain Worklist Community Detail service.

**Table 14–15 SOA Domain - Asserting Party for Worklist Community Detail**

| Parameter   | Value   | Description   |
|-------------|---------|---|
| Enabled     | Checked | <p>Specifies whether this Asserting Party can be used to obtain SAML assertions</p>                                 |
| Description |         | <p>A short description of this Asserting Party (for example, <code>WebCenter Spaces for Worklist Detail</code>)</p> |

**Table 14–15 (Cont.) SOA Domain - Asserting Party for Worklist Community Detail**

| Parameter                      | Value  | Description   |
|--------------------------------|--|---|
| Target URL                     |  | The target URL of this SAML Asserting Party (for example, <code>http://example.com:8888/webcenter</code> )  |
| POST Signing Certificate alias |  | The alias of the certificate trusted for verifying signatures on SAML protocol elements from this Asserting Party (for example, <code>testalias</code> ). Must be set when using Browser/POST profile.  |
| Source Site Redirect URIs      | <code>/workflow/WebCenterWorklistDetail/faces/adf.task-flow</code> | An optional set of URIs from which unauthenticated users will be redirected to the configured ITS URL. If set, the <code>IntersiteTransferURL</code> must also be set.<br><br><b>Note:</b> Based on this setting, when you first access the destination site, you are redirected to the configured ITS URL (which in this case is within the source application), your session is established with the source application and then redirected to the destination site.  |
| Source Site ITS URL            |  | The Intersite Transfer Service (ITS) URL of the SAML Source Site for this Asserting Party (for example, <code>http://example.com:8888/webcenter/samlits/its</code> ).<br><br>Used with SSO profiles only, to support the destination site first scenario, whereby a user tries to access a destination site URL prior to being authenticated and is redirected to the source site to be authenticated and obtain a SAML assertion. The Redirect URIs attribute must also be configured for source-site redirection to work.<br><br><b>Note:</b> If you check <b>ITS requires SSL</b> in Source Site Federation Services, you must also change the Source Site ITS URL to use HTTPS and the server's SSL port. |
| Source Site ITS parameters     | <code>RPID=rp_00001</code>   | Optionally, zero or more query parameters, of the form <code>name=value</code> , that will be added to the ITS URL when redirecting to the source site. In this case <code>rp_00002</code> is the relying party ID for the Worklist Detail application specified in the SAML Credential Mapping provider for the WebCenter domain, which provides the destination site details. For more information, see <a href="#">Table 14–5, "Relying Party Settings for Worklist Community Detail"</a> .  |
| Issuer URI                     |  | The issuer URI of the SAML Authority issuing assertions for this SAML Asserting Party (for example, <code>http://www.example.com/webcenter</code> ).  |
| Signature Required             | Checked  | If checked, assertions must be signed. If unchecked, signature elements are not required, but will be verified if present.  |

**Table 14–15 (Cont.) SOA Domain - Asserting Party for Worklist Community Detail**

| Parameter                           | Value | Description   |
|-------------------------------------|-------|---|
| Assertion Signing Certificate alias |       | The alias of the certificate trusted for verifying signatures on assertions from this Asserting Party (for example, <code>testalias</code> ). This must be set if <b>Signature Required</b> is checked. The certificate must also be registered in the SAML Identity Asserter's certificate registry. |

- Change domains to the SOA domain and repeat steps 1 - 11 using the settings shown in [Table 14–16](#) to configure the Asserting Party for the SOA domain Worklist SDP service. For more information see [Table 14–6, "Relying Party Settings for Worklist SDP"](#) and [Table 14–7, "Relying Party Settings for Worklist Integration"](#).

**Table 14–16 SOA Domain - Asserting Party for Worklist SDP**

| Parameter                      | Value   | Description  |
|--------------------------------|---|--|
| Enabled                        | Checked   | Specifies whether this Asserting Party can be used to obtain SAML assertions.  |
| Description                    |   | A short description of this Asserting Party (for example, <code>WebCenter Spaces for Worklist SDP</code> )   |
| Target URL                     |   | The target URL of this SAML Asserting Party (for example, <code>http://example.com:8888/webcenter</code> )   |
| POST Signing Certificate alias |   | The alias of the certificate trusted for verifying signatures on SAML protocol elements from this Asserting Party (for example, <code>testalias</code> ). Must be set when using Browser/POST profile.   |
| Source Site Redirect URIs      | <code>/workflow/sdpmes<br/>sagingsca-ui-wor<br/>klist/faces/adf.<br/>task-flow</code> | An optional set of URIs from which unauthenticated users will be redirected to the configured ITS URL. If set, the <code>IntersiteTransferURL</code> must also be set.<br><br><b>Note:</b> Based on this setting, when you first access the destination site, you are redirected to the configured ITS URL (which in this case is within the source application), your session is established with the source application and then redirected to the destination site. |

**Table 14–16 (Cont.) SOA Domain - Asserting Party for Worklist SDP**

| Parameter                           | Value         | Description   |
|-------------------------------------|---------------|---|
| Source Site ITS URL                 |               | <p>The Intersite Transfer Service (ITS) URL of the SAML Source Site for this Asserting Party (for example, <code>http://example.com:8888/webcenter/samlits/its</code>).</p> <p>Used with SSO profiles only, to support the destination site first scenario, whereby a user tries to access a destination site URL prior to being authenticated and is redirected to the source site to be authenticated and obtain a SAML assertion. The Redirect URIs attribute must also be configured for source-site redirection to work.</p> <p><b>Note:</b> If you check <b>ITS requires SSL</b> in Source Site Federation Services, you must also change the Source Site ITS URL to use HTTPS and the server's SSL port.</p> |
| Source Site ITS parameters          | RPID=rp_00002 | <p>Optionally, zero or more query parameters, of the form <code>name=value</code>, that will be added to the ITS URL when redirecting to the source site. In this case <code>rp_00003</code> is the relying party ID for the Worklist SDP application specified in the SAML Credential Mapping provider of the WebCenter domain, which provides the destination site details.</p> <p>For more information, see <a href="#">Table 14–6, "Relying Party Settings for Worklist SDP"</a>.</p>   |
| Issuer URI                          |               | <p>The issuer URI of the SAML Authority issuing assertions for this SAML Asserting Party (for example, <code>http://www.example.com/webcenter</code>).</p>  |
| Signature Required                  | Checked       | <p>If true, assertions must be signed. If false, signature elements are not required, but will be verified if present.</p>  |
| Assertion Signing Certificate alias |               | <p>The alias of the certificate trusted for verifying signatures on assertions from this Asserting Party (for example, <code>testalias</code>). This must be set if <b>Signature Required</b> is checked. The certificate must also be registered in the SAML Identity Asserter's certificate registry.</p>   |

16. Change domains to the SOA domain and repeat steps 1 - 11 using the settings shown in [Table 14–17](#) to configure the Asserting Party for the SOA domain Worklist Community Integration service.

**Table 14–17 In SOA Domain, Asserting party For Worklist Integration**

| Parameter   | Value                             | Description  |
|-------------|-----------------------------------|--|
| Enabled     | Checked                           | Specifies whether this Asserting Party can be used to obtain SAML assertions                               |
| Description | WebCenter Spaces for Worklist SDP | A short description of this Asserting Party (for example, <code>WebCenter Spaces for Worklist SDP</code> ) |

**Table 14–17 (Cont.) In SOA Domain, Asserting party For Worklist Integration**

| Parameter                      | Value  | Description   |
|--------------------------------|--|---|
| Target URL                     |  | The target URL of this SAML Asserting Party (for example, <code>http://example.com:8888/webcenter</code> )  |
| POST Signing Certificate alias |  | The alias of the certificate trusted for verifying signatures on SAML protocol elements from this Asserting Party (for example, <code>testalias</code> ). Must be set when using Browser/POST profile.  |
| Source Site Redirect URIs      | <p><code>/integration/worklistapp/ssologin</code></p> <p><code>/integration/worklistapp/faces/home.jspx</code></p> | <p>An optional set of URIs from which unauthenticated users will be redirected to the configured ITS URL. If set, the <code>IntersiteTransferURL</code> must also be set.</p> <p><b>Note:</b> Based on this setting, when you first access the destination site, you are redirected to the configured ITS URL (which in this case is within the source application), your session is established with the source application and then redirected to the destination site.</p>   |
| Source Site ITS URL            |  | <p>The Intersite Transfer Service (ITS) URL of the SAML Source Site for this Asserting Party (for example, <code>http://example.com:8888/webcenter/samlits/its</code>).</p> <p>Used with SSO profiles only, to support the destination site first scenario, whereby a user tries to access a destination site URL prior to being authenticated and is redirected to the source site to be authenticated and obtain a SAML assertion. The Redirect URIs attribute must also be configured for source-site redirection to work.</p> <p><b>Note:</b> If you check <b>ITS requires SSL</b> in Source Site Federation Services, you must also change the Source Site ITS URL to use HTTPS and the server's SSL port.</p> |
| Source Site ITS parameters     | <code>RPID=rp_00003</code>   | <p>Optionally, zero or more query parameters, of the form <code>name=value</code>, that will be added to the ITS URL when redirecting to the source site. In this case <code>rp_00004</code> is the relying party ID for the Worklist Integration application specified in the SAML Credential Mapping provider of the WebCenter domain, which provides the destination site details.</p> <p>For more information, see <a href="#">Table 14–7, "Relying Party Settings for Worklist Integration"</a>.</p>   |
| Issuer URI                     |  | The issuer URI of the SAML Authority issuing assertions for this SAML Asserting Party (for example, <code>http://www.example.com/webcenter</code> ).  |
| Signature Required             | Checked  | If true, assertions must be signed. If false, signature elements are not required, but will be verified if present.   |



**Table 14–17 (Cont.) In SOA Domain, Asserting party For Worklist Integration**

| Parameter                           | Value | Description   |
|-------------------------------------|-------|---|
| Assertion Signing Certificate alias |       | The alias of the certificate trusted for verifying signatures on assertions from this Asserting Party (for example, <code>testalias</code> ). This must be set if <b>Signature Required</b> is checked. The certificate must also be registered in the SAML Identity Asserter's certificate registry. |

### 14.7.3.2.7 Configuring Destination Site Federation Services

This section describes how to configure the Destination Site Federation Services for the Wiki service, RSS, and the Worklist service on the SOA domain.

To configure the Destination Site Federation Services:

1. Log in to the WLS Administration Console.  
For information on logging into the WLS Administration Console, see [Section 1.12.2, "Oracle WebLogic Server Administration Console"](#).
2. On the Domain Structure pane, expand the **Environment** node and click **Servers**.  
The Summary of Servers page displays (see [Figure 14–116](#)).

**Figure 14–116 Summary of Servers Page**

Summary of Servers

**Configuration** Control

A server is an instance of WebLogic Server that runs in its own Java Virtual Machine (JVM) and has its own configuration.  
This page summarizes each server that has been configured in the current WebLogic Server domain.

Customize this table

**Servers (Filtered - More Columns Exist)**

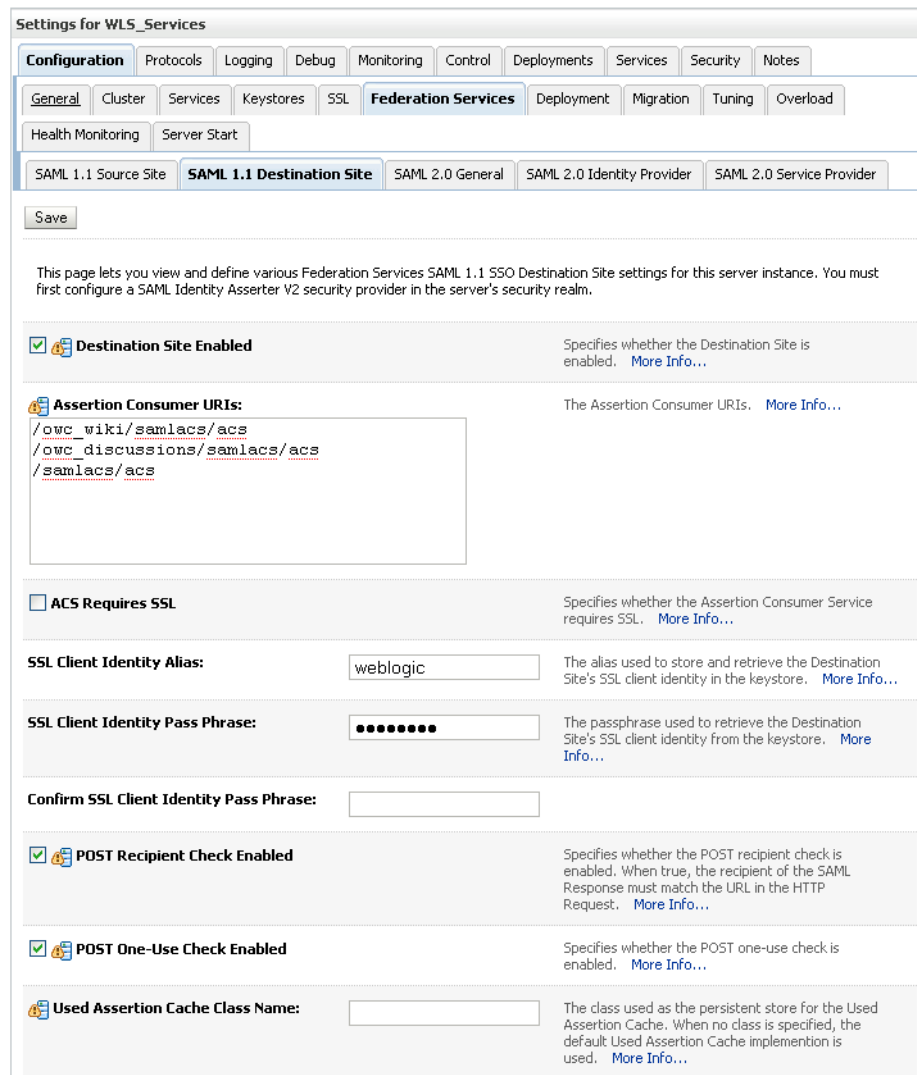
New Clone Delete Showing 1 to 4 of 4 Previous | Next

| <input type="checkbox"/> | Name               | Cluster | Machine   | State   | Health | Listen Port |
|--------------------------|--------------------|---------|-----------|---------|--------|-------------|
| <input type="checkbox"/> | AdminServer(admin) |         |           | RUNNING | OK     | 7001        |
| <input type="checkbox"/> | WLS_Portlet        |         | IR12stage | RUNNING | OK     | 8889        |
| <input type="checkbox"/> | WLS_Services       |         | IR12stage | RUNNING | OK     | 8890        |
| <input type="checkbox"/> | WLS_Spaces         |         | IR12stage | RUNNING | OK     | 8888        |

New Clone Delete Showing 1 to 4 of 4 Previous | Next

3. Click `WLS_Services` (the managed server where the Wiki service and Discussions service are deployed) and open the Configuration tab.
4. Open the Federation Services tab and the SAML 1.1 Destination Site subtab.  
The SAML 1.1 Destination Site Settings pane displays (see [Figure 14–117](#)).

**Figure 14–117 SAML 1.1 Destination Site Settings Pane (Wiki and Discussions)**



5. Configure the SAML destination site attributes for the Wiki and Discussions applications as shown in [Table 14–18](#).

**Table 14–18 SAML Destination Site Attributes (Wiki and Discussions)**

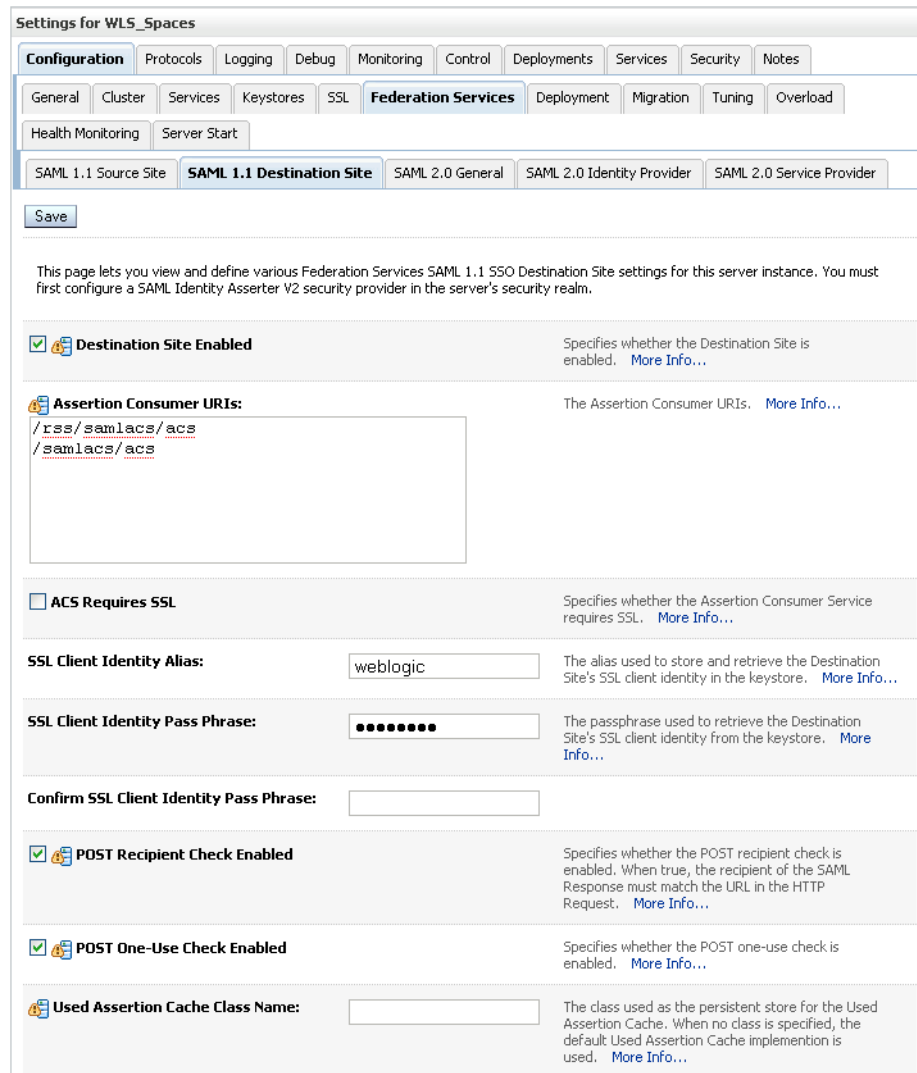
| Parameter                | Value     | Description   |
|--------------------------|-----------|---|
| Destination Site Enabled | Checked   | Specifies whether the Destination Site is enabled.  |
| ACS Requires SSL         | Unchecked | Specifies whether the Assertion Consumer Service requires SSL. If checked, then ensure that the ACS URL specified in the Credential Mapper's relying party uses HTTPS and target server's SSL port. |

**Table 14–18 (Cont.) SAML Destination Site Attributes (Wiki and Discussions)**

| Parameter                    | Value   | Description   |
|------------------------------|---|---|
| Assertion Consumer URIs      | /owc_wiki/samlacs/acs<br>/owc_discussions/samlacs/acs<br>[add on top, leave rest as is] | The Assertion Consumer URIs. In this case, we have chosen for the ACS to reside within the target app so that it uses the same login cookie.    |
| POST Recipient Check Enabled | Checked   | Specifies whether the POST recipient check is enabled. When checked, the recipient of the SAML Response must match the URL in the HTTP Request. |
| POST One use Check Enabled   | Checked   | Specifies whether the POST one-use check is enabled.  |

6. Click **Save** to save your settings, and restart the `WLS_Services` server so that they take effect.
7. From the Domain Structure pane, expand the **Environment** node and click **Servers**.
8. Click `WLS_Spaces` (the managed server where RSS is deployed) and open the Configuration tab.
9. Open the Federation Services tab and the SAML 1.1 Destination Site subtab. The SAML 1.1 Destination Site Settings pane displays (see [Figure 14–118](#)).

**Figure 14–118 SAML 1.1 Destination Site Settings Pane (RSS)**



10. Configure the SAML destination site attributes for RSS as shown in [Table 14–19](#).

**Table 14–19 SAML Destination Site Attributes (RSS)**

| Parameter                | Value  | Description   |
|--------------------------|--|---|
| Destination Site Enabled | Checked  | Specifies whether the Destination Site is enabled.  |
| ACS Requires SSL         | Unchecked  | Specifies whether the Assertion Consumer Service requires SSL. If checked, then ensure that ACS URL specified in Credential Mapper's relying party uses https and target server's SSL port. |
| Assertion Consumer URIs  | /rss/samlacs/acs<br>(add on top, leave rest as is) | The Assertion Consumer URIs. In this case, we have chosen for the ACS to reside within the target app so that it uses the same login cookie.  |

**Table 14–19 (Cont.) SAML Destination Site Attributes (RSS)**

| Parameter                    | Value   | Description  |
|------------------------------|---------|--|
| POST Recipient Check Enabled | Checked | Specifies whether the POST recipient check is enabled. When true, the recipient of the SAML Response must match the URL in the HTTP Request. |
| POST One use Check Enabled   | Checked | Specifies whether the POST one-use check is enabled.   |

11. Click **Save** to save your settings, and restart the `WSL_Spaces` server so that they take effect.
12. Navigate to the SOA domain and then to `soa_server1`, or the managed server where the Worklist applications are deployed.
13. Follow the same steps as above to open the SAML 1.1 Destination Site subtab.  
The SAML 1.1 Destination Site Settings pane displays (see [Figure 14–119](#)).

**Figure 14–119 SAML 1.1 Destination Site Settings Pane (Worklist Detail and SDP)**

Settings for soa\_server1

Configuration Protocols Logging Debug Monitoring Control Deployments Services Security Notes

General Cluster Services Keystores SSL **Federation Services** Deployment Migration Tuning Overload

Health Monitoring Server Start

SAML 1.1 Source Site **SAML 1.1 Destination Site** SAML 2.0 General SAML 2.0 Identity Provider SAML 2.0 Service Provider

Save

This page lets you view and define various Federation Services SAML 1.1 SSO Destination Site settings for this server instance. You must first configure a SAML Identity Asserter V2 security provider in the server's security realm.

**Destination Site Enabled** Specifies whether the Destination Site is enabled. [More Info...](#)

**Assertion Consumer URIs:** The Assertion Consumer URIs. [More Info...](#)

```

/workflow/WebCenterWorklistDetail
/samlacs/acs
/workflow/sdpmessagingsca-ui-worklist
/samlacs/acs
/integration/worklistapp/samlacs/acs
/samlacs/acs
    
```

**ACS Requires SSL** Specifies whether the Assertion Consumer Service requires SSL. [More Info...](#)

**SSL Client Identity Alias:**  The alias used to store and retrieve the Destination Site's SSL client identity in the keystore. [More Info...](#)

**SSL Client Identity Pass Phrase:**  The passphrase used to retrieve the Destination Site's SSL client identity from the keystore. [More Info...](#)

**Confirm SSL Client Identity Pass Phrase:**

**POST Recipient Check Enabled** Specifies whether the POST recipient check is enabled. When true, the recipient of the SAML Response must match the URL in the HTTP Request. [More Info...](#)

**POST One-Use Check Enabled** Specifies whether the POST one-use check is enabled. [More Info...](#)

14. Configure the SAML 1.1 Destination Site attributes for Worklist Detail and SDP as shown in [Table 14–20](#).

**Table 14–20 SOA Domain - SAML Destination Site Attributes (Worklist Detail and SDP)**

| Parameter                    | Value   | Description   |
|------------------------------|---|---|
| Destination Site Enabled     | Checked   | Specifies whether the Destination Site is enabled.  |
| ACS Requires SSL             | Unchecked   | Specifies whether the Assertion Consumer Service requires SSL. If checked, then ensure that ACS URL specified in Credential Mapper's relying party uses HTTPS and the target server's SSL port. |
| Assertion Consumer URIs      | /workflow/WebCenterWorklistDetail/samlacs/acs<br><br>/workflow/sdpmesagingsca-ui-worklist/samlacs/acs<br><br>/integration/worklistapp/samlacs/acs<br><br>(add on top, leave rest as is) | The Assertion Consumer URIs. In this case, we have chosen for the ACS to reside within the target app so that it uses the same login cookie.  |
| POST Recipient Check Enabled | Checked   | Specifies whether the POST recipient check is enabled. When checked, the recipient of the SAML Response must match the URL in the HTTP Request.   |
| POST One use Check Enabled   | Checked   | Specifies whether the POST one-use check is enabled.  |

15. Click **Save** to save your settings.

16. Restart the SOA managed server.

#### 14.7.3.2.8 Checking Your Configuration

The last step in the process is to check that your single sign-on configuration is working. To do that:

1. Check that when you try to access the Wiki and RSS applications independently, you are taken to the WebCenter Spaces login page (source site) and then directed to the URL you were trying to access.
2. Now log into WebCenter Spaces and check that you're not challenged for credentials when:
  - You access the Wiki from a group space
  - You access RSS from a list task flow
  - You click **Forum Administration** from **Group Space Settings > Services > Discussions** (assuming this service is provisioned for the group space)
  - You click a Forum from Group Space Settings from Discussions

#### 14.7.3.2.9 Configuring the Discussions Server for SAML SSO

To configure the discussions server for SAML single sign-on, be sure to perform these steps:

1. Deploy the SSO-enabled discussions server as described in [Section 14.7.1.7.2, "Deploying the Discussions Server"](#)
2. Configure a relying party for the Discussions application as described in [Section 14.7.3.2.4, "Configuring a Relying Party"](#)
3. Configure an asserting party for the Discussions application as described in [Section 14.7.3.2.6, "Configuring the SAML Identity Assertion Provider"](#).
4. Configure the Discussions application in the destination site federation services as described in [Section 14.7.3.2.7, "Configuring Destination Site Federation Services"](#)

## 14.7.4 Configuring SSO with Microsoft Clients

This section describes how to set up single sign-on (SSO) with Microsoft clients, using Windows authentication based on the Simple and Protected Negotiate (SPNEGO) mechanism and the Kerberos protocol, together with the WebLogic Negotiate Identity Assertion provider for the WebCenter Spaces application. This SSO approach enables Microsoft clients (such as browsers), authenticated in a Windows domain using Kerberos, to be transparently authenticated to web applications (such as WebCenter Spaces) in a WebLogic domain based on the same credentials, and without the need to type in their password again.

Cross-platform authentication is achieved by emulating the negotiate behavior of native Windows-to-Windows authentication services that use the Kerberos protocol. In order for cross-platform authentication to work, non-Windows servers (in this case, WebLogic Server) need to parse SPNEGO tokens in order to extract Kerberos tokens, which are then used for authentication.

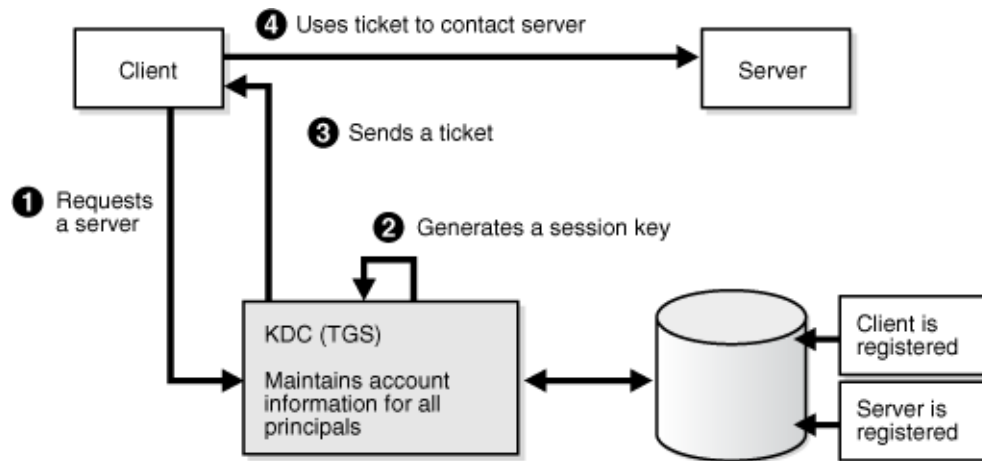
### 14.7.4.1 Microsoft Client SSO Concepts

#### Understanding Kerberos

Kerberos is a secure method for authenticating a request for a service in a network. The Kerberos protocol comprises three parties: a client, a server and a trusted third party to mediate between them, known as the KDC (Key Distribution Center). Under Kerberos, a server allows a user to access its service if the user can provide the server a Kerberos ticket that proves its identity. Both the user and the service are required to have keys registered with the KDC.

The diagram below describes the basic exchanges that must take place before a client connects to a server.

**Figure 14–120 Connecting to a Server Through a Key Distribution Center**



This diagram shows how clients connect to a server through a Key Distribution Center.

\*\*\*\*\*

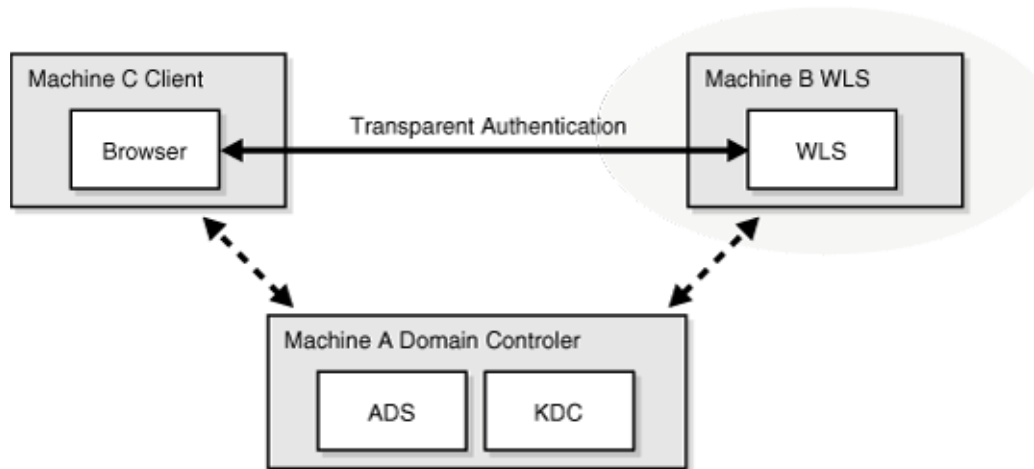
**Understanding SPNEGO**

SPNEGO (Simple and Protected GSSAPI Negotiation Mechanism) is a GSSAPI "pseudo mechanism" that is used to negotiate one of a number of possible real mechanisms. SPNEGO is used when a client application wants to authenticate to a remote server, but neither end is sure what authentication protocols the other supports. The pseudo-mechanism uses a protocol to determine what common GSSAPI mechanisms are available, selects one, and then dispatches all further security operations to it. This can help organizations deploy new security mechanisms in a phased manner.

SPNEGO's most visible use is in Microsoft's HTTP Negotiate authentication extension. The negotiable sub-mechanisms include NTLM and Kerberos, both used in Active Directory.

This feature enables a client browser to access a protected resource on WLS, and to transparently provide the WLS server with authentication information from the Kerberos database using a SPNEGO ticket. The WLS server is able to recognize the ticket and extract the information from it. WLS then uses the information for authentication and grants access to the resource if the authenticated user is authorized to access it. (Kerberos is responsible for authentication only; authorization is still handled by WLS).



**Figure 14-121 SPNEGO-based Authentication**

This diagram shows authentication between a non-WebLogic server and a WebLogic server using SPNEGO.

\*\*\*\*\*

#### 14.7.4.2 System Requirements

To use SSO with Microsoft clients you need:

A host computer with:

- Windows 2000 or later installed
- Fully-configured Active Directory authentication service. Specific Active Directory requirements include:
  - User accounts for mapping Kerberos services
  - Service Principal Names (SPNs) for those accounts
  - Key tab files created and copied to the start-up directory in the WebLogic Server domain
- WebLogic Server installed and configured properly to authenticate through Kerberos, as described in this section

Client systems with:

- Windows 2000 Professional SP2 or later installed
- One of the following types of clients:
  - A properly configured Internet Explorer browser. Internet Explorer 6.01 or later is supported.
  - .NET Framework 1.1 and a properly configured Web Service client.

---

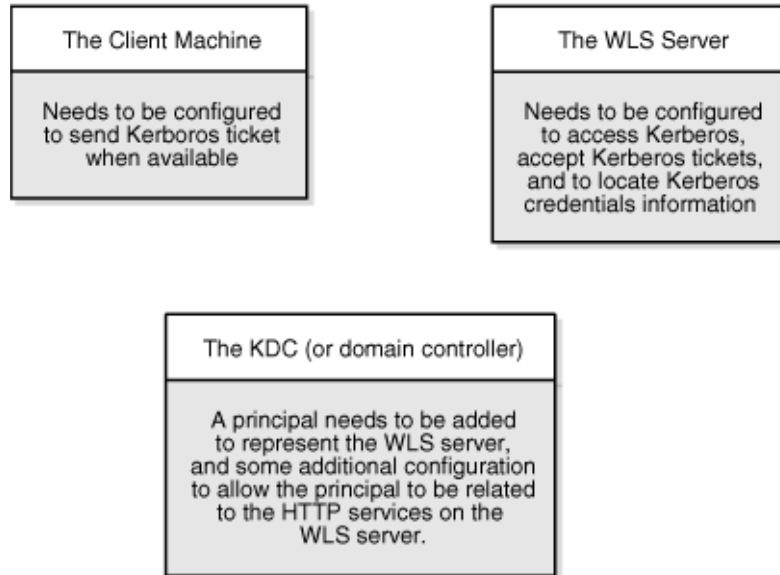
**Note:** Clients must be logged on to a Windows 2000 domain and have Kerberos credentials acquired from the Active Directory server in the domain. Local logons will not work.

---

### 14.7.4.3 Configuring SSO with Microsoft Clients

Configuring SSO with Microsoft clients requires configuring the Microsoft Active Directory, the client, and the WebLogic Server domain shown in [Figure 14–122](#). For detailed configuration steps and troubleshooting, see "Configuring Single Sign-On with Microsoft Clients" in *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

**Figure 14–122 Configuring SSO with Microsoft Clients**



To configure Microsoft clients for SSO:

1. Configure your network domain to use Kerberos.
2. Create a Kerberos identification for WebLogic Server.
  - a. Create a user account in the Active Directory for the host on which WebLogic Server is running.
  - b. Create a Service Principal Name for this account.
  - c. Create a user mapping and keytab file for this account.
3. Choose a Microsoft client (in this case Internet Explorer) and configure it to use Windows Integrated authentication.
4. Set up the WebLogic Server domain (`wc_domain` in this case) to use Kerberos authentication.
  - a. Create a JAAS login file that points to the Active Directory server in the Microsoft domain and the keytab file created in Step 2.
  - b. Configure a Negotiate Identity Assertion provider in the WebLogic Server security realm (see [Section 14.7.4.3.1, "Configuring the Negotiate Identity Assertion Provider"](#))
  - c. Configure the WLS domain to use the Active Directory Authenticator so that the WebLogic domain uses the same Active Directory of the domain as the identity store. You could also use a different identity store and match the users in this store with the Active Directory users of your domain, but using the Active Directory authenticator is recommended as maintaining two different

identity stores risks them getting out of sync. See [Section 14.7.4.3.2, "Configuring an Active Directory Authentication Provider"](#))

---

**Caution:** Ensure that only the identity store is configured for Active Directory. The policy and credential stores are not certified for Active Directory.

---

5. Start the WebLogic Servers (Administration Server and managed servers) using specific start-up arguments. Repeat steps 4 and 5 for the SOA Domain to enable single sign-on for SOA applications.
6. Configure WebCenter Spaces (see [Section 14.7.4.3.3, "Configuring WebCenter Spaces"](#)).

#### 14.7.4.3.1 Configuring the Negotiate Identity Assertion Provider

This section provides instructions for creating and configuring a Negotiate Identity Assertion provider. The Negotiate Identity Assertion provider enables single sign-on (SSO) with Microsoft clients. The identity assertion provider decodes Simple and Protected Negotiate (SPNEGO) tokens to obtain Kerberos tokens, validates the Kerberos tokens, and maps them to WebLogic users. The Negotiate Identity Assertion provider uses the Java Generic Security Service (GSS) Application Programming Interface (API) to accept the GSS security context via Kerberos.

To configure the Negotiate Identity Assertion provider:

1. Log in to the WLS Administration Console.

For information on logging into the WLS Administration Console, see [Section 1.12.2, "Oracle WebLogic Server Administration Console"](#).

2. From the Domain Structure pane, click **Security Realms**.

The Summary of Security Realms pane displays (see [Figure 14-123](#)).

**Figure 14-123 Summary of Security Realms Pane**

**Summary of Security Realms**

A security realm is a container for the mechanisms—including users, groups, security roles, security policies, and security providers—that are used to protect WebLogic resources. You can have multiple security realms in a WebLogic Server domain, but only one can be set as the default (active) realm.

This Security Realms page lists each security realm that has been configured in this WebLogic Server domain. Click the name of the realm to explore and configure that realm.

[Customize this table](#)

Realms(Filtered - More Columns Exist)

| <input type="checkbox"/> | Name ↕  | Default Realm |
|--------------------------|---------|---------------|
| <input type="checkbox"/> | myrealm | true          |

New Delete Showing 1 to 1 of 1 Previous | Next

3. Click your security realm.

The Settings page for the security realm displays (see [Figure 14–124](#)).

**Figure 14–124 Security Realm Settings Page**

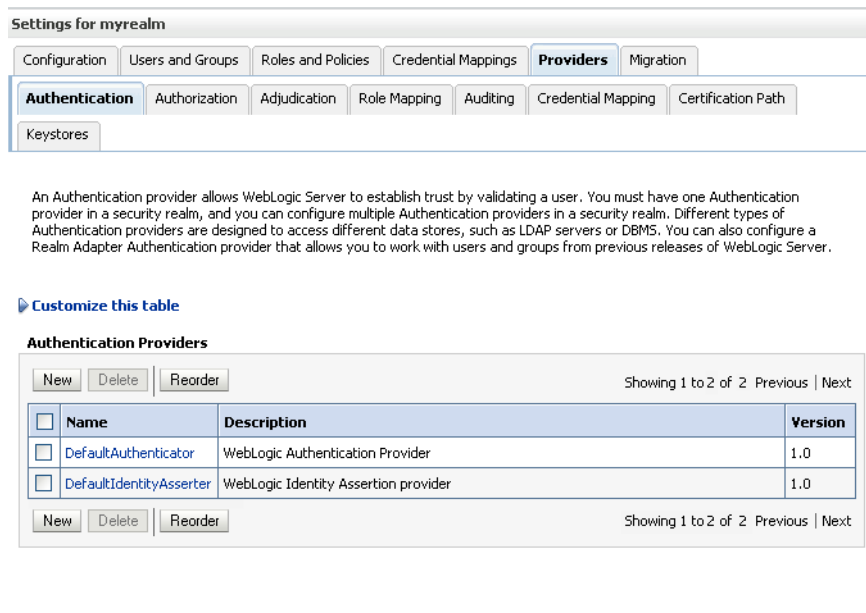
The screenshot shows the 'Settings for myrealm' page. At the top, there are tabs for 'Configuration', 'Users and Groups', 'Roles and Policies', 'Credential Mappings', 'Providers', and 'Migration'. Below these are sub-tabs for 'General', 'RDBMS Security Store', 'User Lockout', and 'Performance'. A 'Save' button is located at the top left. The main content area contains the following settings:

- Name:** myrealm. Description: The name of this security realm. [More Info...](#)
- Security Model Default:** DD Only. Description: Specifies the default security model for Web applications or EJBs that are secured by this security realm. You can override this default during deployment. [More Info...](#)
- Combined Role Mapping Enabled:** . Description: Determines how the role mappings in the Enterprise Application, Web application, and EJB containers interact. This setting is valid only for Web applications and EJBs that use the Advanced security model and that initialize roles from deployment descriptors. [More Info...](#)
- Use Authorization Providers to Protect JMX Access:** . Description: Configures the WebLogic Server MBean servers to use the security realm's Authorization providers to determine whether a JMX client has permission to access an MBean attribute or invoke an MBean operation. [More Info...](#)

At the bottom, there is an 'Advanced' section header and another 'Save' button.

4. Open the Providers tab and select the Authentication subtab.  
The Authentication Settings pane displays (see [Figure 14–125](#)).

**Figure 14–125 Authentication Settings Pane**



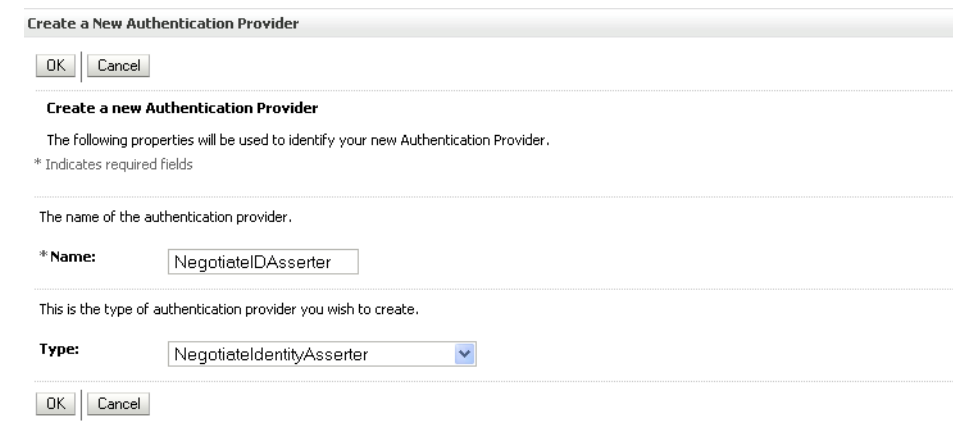
This screenshot shows the Authentication Settings pane.

\*\*\*\*\*

**5. Click New.**

The Create a New Authentication Provider pane displays (see [Figure 14–126](#)).

**Figure 14–126 Create a New Authentication Provider Pane**



**6. Enter a Name for the identity asserter, and select NegotiateIdentityAsserter as the Type.**

**7. Click OK.**

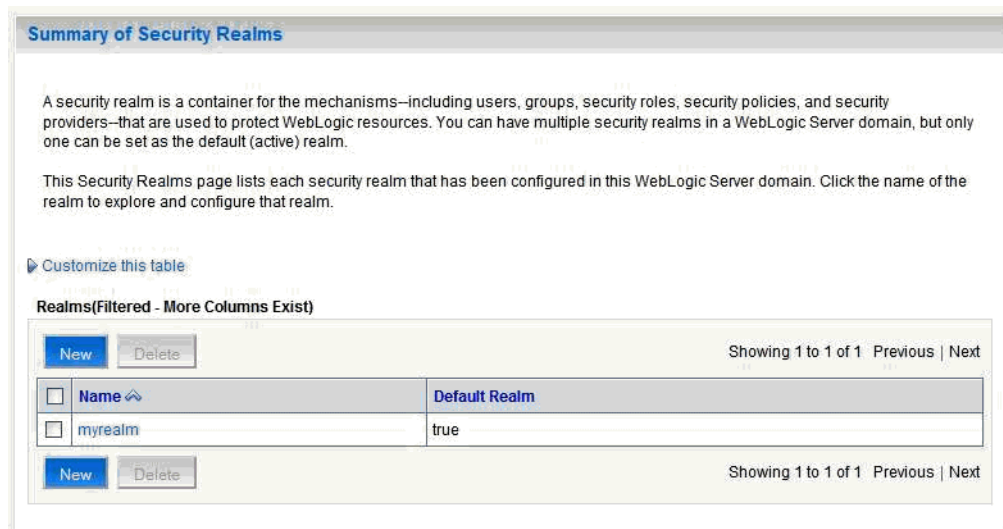
**14.7.4.3.2 Configuring an Active Directory Authentication Provider**

Follow the steps below to configure an Active Directory authentication provider using the WebLogic Administration Console.

To configure an Active Directory Authentication provider:

1. Log in to the WLS Administration Console.  
 For information on logging into the WLS Administration Console, see [Section 1.12.2, "Oracle WebLogic Server Administration Console"](#).
2. From the Domain Structure pane, click **Security Realms**.  
 The Summary of Security Realms pane displays (see [Figure 14–127](#)).

**Figure 14–127 Summary of Security Realms Pane**



3. Click your security realm.  
 The Settings page for the security realm displays (see [Figure 14–128](#)).

**Figure 14–128 Security Realm Settings Page**

**Settings for myrealm**

Configuration
Users and Groups
Roles and Policies
Credential Mappings
Providers
Migration

General
RDBMS Security Store
User Lockout
Performance

Save

Use this page to configure the general behavior of this security realm.

**Note:**  
If you are implementing security using JACC (Java Authorization Contract for Containers as defined in JSR 115), you must use the DD Only security model. Other WebLogic Server models are not available and the security functions for Web applications and EJBs in the Administration Console are disabled.

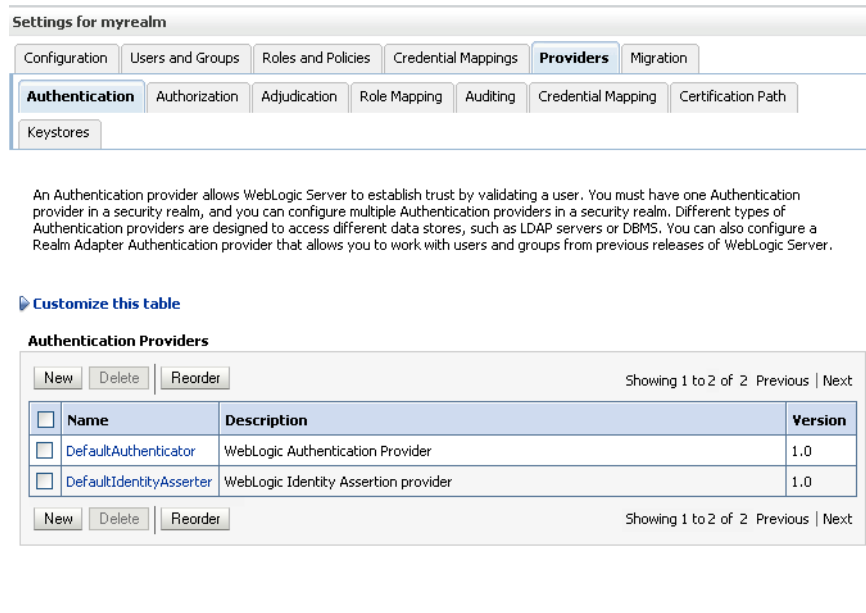
|   |                                      |   |
|---|--------------------------------------|---|
| <b>Name:</b>  | myrealm                              | The name of this security realm. <a href="#">More Info...</a>   |
| <b>Security Model Default:</b>  | <input type="text" value="DD Only"/> | Specifies the default security model for Web applications or EJBs that are secured by this security realm. You can override this default during deployment. <a href="#">More Info...</a>  |
| <input checked="" type="checkbox"/> <b>Combined Role Mapping Enabled</b>          |                                      | Determines how the role mappings in the Enterprise Application, Web application, and EJB containers interact. This setting is valid only for Web applications and EJBs that use the Advanced security model and that initialize roles from deployment descriptors. <a href="#">More Info...</a> |
| <input type="checkbox"/> <b>Use Authorization Providers to Protect JMX Access</b> |                                      | Configures the WebLogic Server MBean servers to use the security realm's Authorization providers to determine whether a JMX client has permission to access an MBean attribute or invoke an MBean operation. <a href="#">More Info...</a>   |

▶ Advanced

Save

4. Open the Providers tab and select the Authentication subtab.  
The Authentication Settings pane displays (see [Figure 14–129](#)).

**Figure 14–129 Authentication Settings Pane**



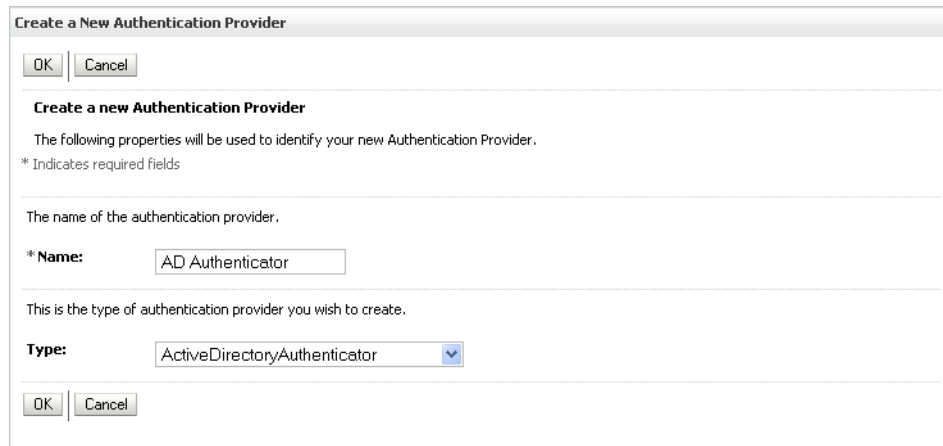
This screenshot shows the Authentication Settings pane.

\*\*\*\*\*

5. Click **New**.

The Create a New Authentication Provider pane displays (see [Figure 14–130](#)).

**Figure 14–130 Create a New Authentication Provider Pane**



6. Enter a **Name** for the authentication provider, and select `ActiveDirectoryAuthenticator` as the **Type**.
7. Click **OK**.
8. Click on the authentication provider you just created in the list of providers.  
The Settings page for the provider displays (see [Figure 14–131](#)).



**Figure 14–131 Provider Settings Page**

Settings for AD Authenticator

Configuration Performance

Common Provider Specific

Save

Use this page to define the common configuration of this Active Directory Authentication provider.

|               |  |   |
|---------------|--|---|
| Name:         | AD Authenticator                           | The name of this Active Directory Authentication provider. <a href="#">More Info...</a>                             |
| Description:  | Provider that performs LDAP authentication | A short description of this Active Directory Authentication provider. <a href="#">More Info...</a>                  |
| Version:      | 1.0  | The version number of this Active Directory Authentication provider. <a href="#">More Info...</a>                   |
| Control Flag: | SUFFICIENT                                 | Specifies how this Realm Adapter Authentication provider fits into the login sequence. <a href="#">More Info...</a> |

Save

9. Open the Configuration tab and the Common subtab.
10. Set the Control Flag to SUFFICIENT and click **Save**.

---

**Note:** The Control Flag settings of any other authenticators must also be changed to SUFFICIENT. If there is a pre-existing Default Authenticator that has its Control Flag set to REQUIRED, it must be changed to SUFFICIENT.

---

11. Open the Provider Specific subtab.  
The Provider Specific Settings pane displays (see [Figure 14–132](#)).

**Figure 14–132 Provider Specific Settings Pane**

**Settings for AD Authenticator**

Configuration Performance

Common **Provider Specific**

Save

Use this page to define the provider specific configuration for this Active Directory Authentication provider.

---

**Connection**

**Host:**  The host name or IP address of the LDAP server. [More Info...](#)

**Port:**  The port number on which the LDAP server is listening. [More Info...](#)

**Principal:**  The Distinguished Name (DN) of the LDAP user that WebLogic Server should use to connect to the LDAP server. [More Info...](#)

**Credential:**  The credential (usually a password) used to connect to the LDAP server. [More Info...](#)

**Confirm Credential:**

**SSLEnabled** Specifies whether the SSL protocol should be used when connecting to the LDAP server. [More Info...](#)

---

**Users**

**User Base DN:**  The base distinguished name (DN) of the tree in the LDAP directory that contains users. [More Info...](#)

**All Users Filter:**  If the attribute (user object class) is not specified (that is, if the attribute is null or empty), a default search filter is created based on the user schema. [More Info...](#)

**User From Name Filter:**  If the attribute (user name attribute and user object class) is not specified (that is, if the attribute is null or empty), a default search filter is created based on the user schema. [More Info...](#)

**User Search Scope:**  Specifies how deep in the LDAP directory tree the LDAP Authentication provider should search for users. [More Info...](#)

**User Name Attribute:**  The attribute of an LDAP user object that specifies the name of the user. [More Info...](#)

**User Object Class:**  The LDAP object class that stores users. [More Info...](#)

12. Complete the fields as shown in the table below. Leave the rest of the fields set to their default values.

**Table 14–21 Active Directory Authenticator Settings**

| Parameter              | Value                        | Description  |
|------------------------|------------------------------|--|
| Host:                  |                              | The host ID of the LDAP server   |
| Port:                  |                              | The port number of the LDAP server   |
| Principal:             |                              | The LDAP administrator principal   |
| Credential:            |                              |  |
| User Base DN:          |                              | The user search base (for example, OU=spnego unit,DC=admin,DC=oracle,DC=com) |
| User From Name Filter: | (&(cn=%u)(objectclass=user)) |  |
| User Search Scope:     | subtree                      |  |
| User Name Attribute:   | cn                           |  |

**Table 14–21 (Cont.) Active Directory Authenticator Settings**

| Parameter                              | Value                             | Description                                  |
|--|-----------------------------------|--|
| User Search Scope:                     | user                              |  |
| Group Base DN:                         |                                   | The group search base (same as User Base DN) |
| Group From Name Filter:                | (&(cn=%g)(objectclass=group))     |  |
| Group Search Scope:                    | subtree                           |  |
| Static Group Name Attribute:           | cn                                |  |
| Static Group Object Class:             | group                             |  |
| Static Member DN Attribute:            | member                            |  |
| Static Group DN from Member DN Filter: | (&(member=%M)(objectclass=group)) |  |

**13. Click Save.**

**14.** On the Provider Summary page, reorder the providers in the following order, making sure that their Control Flags are set to `SUFFICIENT` where applicable:

1. Negotiate Identity Asserter
2. ActiveDirectoryAuthenticator (SUFFICIENT)
3. DefaultAuthenticator (SUFFICIENT)
4. Other authenticators...

**14.7.4.3.3 Configuring WebCenter Spaces**

Once you have completed the steps for configuring the Negotiate Identity Assertion Provider and Active Directory Authenticator, and all applications on your WebLogic domain are configured for single sign-on with Microsoft clients in the required domain, a final step is required to provide a seamless single-sign-on experience for your users when accessing WebCenter Spaces. There are two options for doing this:

- Turn off public access, by logging into WebCenter Spaces as an administrator and removing view access from the Public role. Once public access has been turned off, accessing the URL `http://host:port/webcenter` will directly take the user to the authenticated view rather than the default public page which has a login section. This is recommended when users will be accessing WebCenter Spaces only using Internet Explorer, and will be confined to the domain where WNA is set up.
- If you need to retain public access to WebCenter Spaces, then the recommendation is to use the `oracle.webcenter.osso.enabled` flag when starting the `WLS_Spaces` server. This flag tells WebCenter Spaces that SSO is being used and no login form should be displayed on the default landing page. A login link is displayed instead that the user can click to invoke the SSO authentication where the user will be automatically logged in. If Firefox is used to access WebCenter Spaces within the Windows network configured for WNA, or any browser is used to access WebCenter Spaces from outside the Windows network domain, the user will see the login page after clicking the Login link.

## 14.8 Configuring WS-Security

This section describes setting up WS-Security for WebCenter Spaces and related components and includes the following subsections:

- [Securing the BPEL Server with WS-Security](#)
- [Securing the Discussions Server with WS-Security](#)
- [Securing Oracle WebLogic Communication Services \(OWLCS\) with WS-Security](#)
- [Securing a WSRP Producer with WS-Security](#)
- [Securing WebCenter Spaces for Applications Consuming Spaces Client APIs with WS-Security](#)

### 14.8.1 Securing the BPEL Server with WS-Security

WebCenter Spaces workflows deployed on a SOA instance invoke the WebCenter client APIs that are deployed on a WebCenter Spaces instance. To enable secure Web services calls between these two instances, the administrator must set up WS-Security as described in this section.

This section includes the following subsections:

- [Generating the Keystores](#)
- [Generating the Keystores When the SOA Server and WebCenter Share the Same Domain](#)
- [Registering the Keystores](#)
- [Updating the Credential Stores](#)

Note that if the SOA server and WebCenter Spaces share the same domain the steps for generating the keystores are different. If the SOA server and WebCenter Spaces are on different domains follow the instructions in [Section 14.8.1.1, "Generating the Keystores"](#); if the SOA server and WebCenter Spaces share the same domain follow the instructions in [Section 14.8.1.2, "Generating the Keystores When the SOA Server and WebCenter Share the Same Domain."](#) The remaining steps for [Registering the Keystores](#) and [Updating the Credential Stores](#) are the same in both cases.

#### 14.8.1.1 Generating the Keystores

This section describes how to generate the keystores, and import the trusted certificates of the WebCenter keystore to the Oracle SOA instance using `webcenter_spaces_ws` as the alias.

This section includes the following subsections:

- [Generating the Keystores in the WebCenter Spaces Keystore](#)
- [Importing the Trusted Certificate of the WebCenter Spaces Keystore to the SOA Keystore](#)
- [Generating a Key Pair in the SOA Instance](#)
- [Exporting the Public Key of the SOA Instance](#)
- [Importing the Trusted Certificate of the SOA Instance in the WebCenter Instance](#)

##### 14.8.1.1.1 Generating the Keystores in the WebCenter Spaces Keystore

For information on how to generate keystores, see [Section 14.8.4.3, "Setting Up the Keystores"](#). In this case, WebCenter is the producer, and BPEL is the consumer.

### 14.8.1.1.2 Importing the Trusted Certificate of the WebCenter Spaces Keystore to the SOA Keystore

After you have created keystores in the WebCenter Spaces instance, import the trusted certificate of the alias `webcenter_spaces_ws` to the SOA instance.

---

**Note:** The alias parameter must always be set to `webcenter_spaces_ws`. If you change the alias, the security setup will not work correctly.

---

To import the trusted certificate in the SOA keystore:

1. Go to `JAVA_HOME/bin/`.
2. Run the following command:

```
keytool -importcert -alias webcenter_spaces_ws -file certificate_file -keystore keystore_name -storepass keystore_password
```

Where:

- `certificate_file` is the file name or path for the WebCenter's certificate file (for example, `webcenter.cer`)
- `keystore_name` is the keystore name in the SOA instance (for example, `bpel.jks`)
- `keystore_password` is the keystore password for the SOA instance's keystore.

#### Example 14-1 Import Trusted Certificate in the SOA Instance

```
keytool -importcert -alias webcenter_spaces_ws -file producer.cer -keystore bpel.jks -storepass password
```

### 14.8.1.1.3 Generating a Key Pair in the SOA Instance

This section describes how to generate a key pair in the SOA instance.

To generate the key pair:

1. Go to `JAVA_HOME/bin/`.
2. Run the following command:

```
keytool -genkeypair -keyalg RSA -dname "bpel_dname" -alias bpel_alias -keypass key_password -keystore keystore -storepass keystore_password -validity days_valid
```

Where:

- `bpel_dname` is dname of the SOA instance (for example, `cn=bpel,dc=example,dc=com`).
- `bpel_alias` is the alias in keystore for the SOA instance (for example, `bpel`).
- `key_password` is the keystore password for the new public key.
- `keystore` is the keystore name for the SOA instance (for example, `bpel.jks`).
- `keystore_password` is the keystore password of the SOA instance's keystore.

- *days\_valid* is the number of days for which the key password is valid (for example, 1024).

**Example 14–2 Generate a Key Pair in the SOA Instance**

```
keytool -genkeypair -keyalg RSA -dname "cn=producer,dc=example,dc=com" -alias bpel  
-keypass password -keystore bpel.jks -storepass welcome1 -validity 1024
```

**14.8.1.1.4 Exporting the Public Key of the SOA Instance**

This section describes how to export public key of the SOA instance.

To export the public key:

1. Go to *JAVA\_HOME/bin/*.
2. Run the following command:

```
keytool -exportcert -v -alias bpel_alias -keystore keystore -storepass  
keystore_password -rfc -file certificate_file
```

Where:

- *bpel\_alias* is the alias in the keystore of the SOA instance (for example, *bpel*).
- *keystore* is the keystore name of the SOA instance (for example, *bpel.jks*).
- *keystore\_password* is the keystore password for the keystore in the SOA instance.
- *certificate\_file* is the file name for the certificate in which the key is to be exported. For example, *bpel.cer*.

**Example 14–3 Export the Public Key of the SOA Instance**

```
keytool -exportcert -v -alias bpel -keystore bpel.jks -storepass password -rfc  
-file bpel.cer
```

**14.8.1.1.5 Importing the Trusted Certificate of the SOA Instance in the WebCenter Instance**

To import the trusted certificate of the SOA instance in the WebCenter instance:

1. Go to *JAVA\_HOME/bin/*.
2. Run the following command:

```
keytool -importcert -alias bpel_alias -file certificate_file -keystore  
keystore_name -storepass keystore_password
```

Where:

- *certificate\_file* is the exported certificate file from the SOA instance (for example, *bpel.cer*).
- *bpel\_alias* is the alias in keystore of the SOA instance (for example, *bpel*).
- *keystore\_name* is the keystore name of the WebCenter instance (for example, *webcenter.jks*).
- *keystore\_password* is the keystore password for keystore in the SOA instance.

**Example 14-4 Import the Trusted Certificate in the WebCenter Instance**

```
keytool -importcert -alias bpel -file bpel.cer -keystore webcenter.jks -storepass
password
```

**14.8.1.2 Generating the Keystores When the SOA Server and WebCenter Share the Same Domain**

This section describes how to generate the keystores and import the trusted certificate of the WebCenter keystore to the Oracle SOA instance using `webcenter_spaces_ws` as the alias when both share the same domain. After generating the producer keystore pair, continue by registering the keystores as shown in [Section 14.8.1.3, "Registering the Keystores,"](#) and updating the Credential Store as shown in [Section 14.8.1.4, "Updating the Credential Stores."](#)

To create the Java keystores for the producer:

1. Go to `JDEV_HOME/jdk/bin` and open a command prompt.
2. Using `keytool`, generate a key pair:

```
keytool -genkeypair -keyalg RSA -dname "producer_dname" -alias producer_alias
-keypass key_password -keystore keystore -storepass keystore_password -validity
days_valid
```

Where:

- `producer_dname` is the name of the producer (for example, `cn=producer,dc=example,dc=com`)
- `producer_alias` is the alias of the producer (for example, `producer`)
- `key_password` is the password for the new public key, (for example, `welcome1`)
- `keystore` is the keystore name, (for example, `producer.jks`)
- `keystore_password` is the keystore password, (for example, `welcome1`)
- `days_valid` is the number of days for which the key password is valid (for example, `365`)

---

**Note:** You must use the `-keyalg` parameter and specify `RSA` as its value as shown above as the default algorithm (DSA) used by `keytool` for generating the key is incompatible with Oracle WebServices Security Manager requirements.

---

**Example 14-5**

```
keytool -genkeypair -keyalg RSA -dname "cn=producer,dc=example,dc=com" -alias
producer -keypass welcome1 -keystore producer.jks -storepass welcome1 -validity
365
```

3. Export the certificate of the producer:

```
keytool -exportcert -v -alias producer_alias -keystore keystore -storepass
keystore_password -rfc -file certificate_file
```

Where:

- `producer_alias` is the alias of the producer (for example, `producer`)
- `keystore` is the keystore name (for example, `producer.jks`)

- *keystore\_password* is the keystore password (for example, `welcome1`)
- *certificate\_file* is the file name for the certificate to export the key to (for example, `producer.cert`)

**Example 14–6**

```
keytool -exportcert -v -alias producer -keystore producer.jks -storepass welcome1
-rfc -file producer.cert
```

4. Import the certificate to the same keystore using the alias **webcenter\_spaces\_ws**. You must use this alias or the end-to-end integration with workflows will fail.

```
keytool -importcert -alias webcenter_spaces_ws -file certificate_file -keystore
keystore -storepass keystore_password
```

Where:

- *certificate\_file* is the file name or path for the producer's certificate file (for example, `./producer/producer.cert`)
- *keystore* is the keystore name (for example, `producer.jks`)
- *keystore\_password* is the keystore password (for example, `welcome1`)

**Example 14–7**

```
keytool -importcert -alias webcenter_spaces_ws -file producer.cert -keystore
producer.jks -storepass welcome1
```

**14.8.1.3 Registering the Keystores**

This section describes how to register keystores in the SOA and WebCenter Spaces instances. This section includes the following subsections:

- [Registering the Keystores in the WebCenter Spaces Instance](#)
- [Registering the Keystores in the SOA Instance](#)

**14.8.1.3.1 Registering the Keystores in the WebCenter Spaces Instance**

Before they can be used, the keystores must also be registered. Follow the steps below to register the keystores in the WebCenter Spaces instance.

To register the keystores in the WebCenter Spaces instance:

1. Change directories to `WEBCENTER_HOME/user_projects/domains/<domain_name>/config/fmwconfig` where the WebCenter instance is installed.
2. Copy the WebCenter keystore that you created earlier, for example, `webcenter.jks`, by running the following command:  

```
cp webcenter.jks .
```
3. In the `jps-config.xml` file, set the keystore location to the name of the keystore (for example, `webcenter.jks`).

```
<serviceInstance name="keystore" provider="keystore.provider"
  location="./webcenter.jks">
  <description>Default JPS Keystore Service</description>
  <property name="keystore.type" value="JKS"/>
  <property name="keystore.csf.map" value="oracle.wsm.security"/>
  <property name="keystore.pass.csf.key" value="keystore-csf-key"/>
```



```
<property name="keystore.sig.csf.key" value="enc-csf-key" />
<property name="keystore.enc.csf.key" value="enc-csf-key" />
```

### 14.8.1.3.2 Registering the Keystores in the SOA Instance

Keystores must be registered before they can be used. You can register keystores using command line, as described in this section or through Fusion Middleware Control, as described in [Section 14.8.4.3.2, "Configuring the Keystores"](#). If you choose to register keystores using Fusion Middleware Control, make sure that property names are identical to those described in this section.

To register keystores using the command line tool:

1. `cd SOA_HOME/user_projects/domains/<domain_name>/config/fmwconfig` where the SOA instance is installed.
2. Copy the SOA keystore that you created earlier, for example, `bpel.jks`, by running the following command:
 

```
cp bpel.jks .
```
3. In the `jps-config.xml` file, set the keystore location to the name of the keystore, for example, `webcenter.jks`.

```
<serviceInstance name="keystore" provider="keystore.provider"
location="./bpel.jks">
  <description>Default JPS Keystore Service</description>
  <property name="keystore.type" value="JKS" />
  <property name="keystore.csf.map" value="oracle.wsm.security" />
  <property name="keystore.pass.csf.key" value="keystore-csf-key" />
  <property name="keystore.sig.csf.key" value="enc-csf-key" />
  <property name="keystore.enc.csf.key" value="enc-csf-key" />
```

### 14.8.1.4 Updating the Credential Stores

After registering the keystores for the SOA and WebCenter instances, you must update the credential store of these instances to add the keystores, signing, encryption keys, and passwords. You can update the credential stores using the `createCred` WLST command or Fusion Middleware Control.

This section includes the following sub sections:

- [Updating the Credential Store in the WebCenter Spaces Instance Using WLST](#)
- [Updating the Credential Store in the WebCenter Spaces Instance Using Fusion Middleware Control](#)
- [Updating the Credential Store in the SOA Instance Using WLST](#)
- [Updating the Credential Store in the SOA Instance Using Fusion Middleware Control](#)

#### 14.8.1.4.1 Updating the Credential Store in the WebCenter Spaces Instance Using WLST

To update the credential store using WLST, see the section "createCred" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*. Use the following example values to add `keystore-csf-key`, `enc-csf-key`, and `sign-csf-key` encryption keys. Before running the command, be sure to back up the `cwallet.sso` file.

#### Example 14–8 keystore-csf-key

```
createCred(map="oracle.wsm.security", key="keystore-csf-key", user="keystore-csf-key
```

```
",password="password",desc="Enc Password")
```

#### **Example 14–9 enc-csf-key**

```
createCred(map="oracle.wsm.security",key="enc-csf-key",user="webcenter",password="password",desc="Enc Password")
```

#### **Example 14–10 sign-csf-key**

```
createCred(map="oracle.wsm.security",key="sign-csf-key",user="webcenter",password="password",desc="Enc Password")
```

### **14.8.1.4.2 Updating the Credential Store in the WebCenter Spaces Instance Using Fusion Middleware Control**

This section describes how to update credential store of the WebCenter Spaces instance using Fusion Middleware Control. Before running the command, be sure to back up the `wallet.sso` file located in the `SOA_HOME/user_projects/domains/<user_domain>/config/fmwconfig` directory.

To update the credential store using Fusion Middleware Control:

1. Open Fusion Middleware Control and log into the target domain.  
For information on logging into Fusion Middleware Control, see [Section 6, "Starting Enterprise Manager Fusion Middleware Control"](#).
2. From the WebLogic Domain menu, select **Security** and then **Credentials**.
3. On the Credentials page, click **Create Map**.
4. In the Create Map dialog, enter `oracle.wsm.security` as the map name. Click **OK**.
5. On the Credentials page, click **Create Key**, to create `keystore-csf-key`.
6. In the Create Key dialog, from the **Select Map** field, select **oracle.wsm.security**.
7. In the **Key** field, enter `keystore-csf-key`.
8. From the **Type** field, select **Password**, if it is not already selected.
9. In the **User Name** field, enter `keystore-csf-key`.
10. In the **Password** field, enter password of the keystore used for the WebCenter instance.
11. Optionally, enter a description and click **OK**.
12. On the Credentials page, click **Create Key**, to create `sign-csf-key`.
13. In the Create Key dialog, in the **Key** field, enter `sign-csf-key`.
14. In the **User Name** field, enter the public key alias of the keystore used in WebCenter instance. For example, `webcenter`.
15. In the **Password** field, enter password of the public key used in the WebCenter instance.
16. Optionally, enter a description and click **OK**.
17. On the Credentials page, click **Create Key**, to create `enc-csf-key`.
18. In the Create Key dialog, in the **Key** field, enter `enc-csf-key`.
19. In the **User Name** field, enter the public key alias of the keystore used in the WebCenter Spaces instance. For example, `webcenter`.

20. In the **Password** field, enter the password of the public key used in the WebCenter instance.
21. Optionally, enter a description and click **OK**.
22. Restart both Administration server and managed servers as described in [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments"](#).

#### 14.8.1.4.3 Updating the Credential Store in the SOA Instance Using WLST

Update the credential store using the WLST `createCred` command. Use the following example values to add `keystore-csf-key`, `enc-csf-key`, and `sign-csf-key` encryption keys.

##### **Example 14–11** *keystore-csf-key*

```
createCred(map="oracle.wsm.security",key="keystore-csf-key",user="keystore-csf-key",password="password",desc="Enc Password")
```

##### **Example 14–12** *enc-csf-key*

```
createCred(map="oracle.wsm.security",key="enc-csf-key",user="bpel",password="password",desc="Enc Password")
```

##### **Example 14–13** *sign-csf-key*

```
createCred(map="oracle.wsm.security",key="sign-csf-key",user="bpel",password="password",desc="Enc Password")
```

#### 14.8.1.4.4 Updating the Credential Store in the SOA Instance Using Fusion Middleware Control

This section describes how to update the credential store in the SOA instance using Fusion Middleware Control.

To update the credential store using Fusion Middleware Control:

1. Open Fusion Middleware Control and log into the target domain.  
For information on logging into Fusion Middleware Control, see [Section 6, "Starting Enterprise Manager Fusion Middleware Control"](#).
2. From the WebLogic Domain menu, select **Security** and then **Credentials**.
3. On the Credentials page, click **Create Map**.
4. In the Create Map dialog, enter `oracle.wsm.security` as the map name. Click **OK**.
5. On the Credentials page, click **Create Key**, to create `keystore-csf-key`.
6. In the Create Key dialog, from the **Select Map** field, select **oracle.wsm.security**.
7. In the **Key** field, enter `keystore-csf-key`.
8. From the **Type** field, select **Password**, if it is not already selected.
9. In the **User Name** field, enter `keystore-csf-key`.
10. In the **Password** field, enter password of the keystore used for the SOA instance.
11. Optionally, enter a description and click **OK**.
12. On the Credentials page, click **Create Key**, to create `sign-csf-key`.

13. In the Create Key dialog, in the **Key** field, enter `sign-csf-key`.
14. In the **User Name** field, enter the public key alias of the keystore used in SOA instance. For example, `bpel`.
15. In the **Password** field, enter password of the public key used in the SOA instance.
16. Optionally, enter a description and click **OK**.
17. On the Credentials page, click **Create Key**, to create `enc-csf-key`.
18. In the Create Key dialog, in the **Key** field, enter `enc-csf-key`.
19. In the **User Name** field, enter the public key alias of the keystore used in SOA instance. For example, `bpel`.
20. In the **Password** field, enter password of the public key used in the SOA instance.
21. Optionally, enter a description and click **OK**.

## 14.8.2 Securing the Discussions Server with WS-Security

By default, the Oracle WebCenter Discussions allows unsecured Web service calls. You can optionally configure Oracle WebCenter Discussions to enable the Web Services Security (WS-Security) trusted authentication. WS-Security establishes a trust relationship between your WebCenter application and Oracle WebCenter Discussions so that your WebCenter application can pass the user identity information to the server without knowing the user's credentials.

To configure WS-Security on the Discussions server side, you must create a keystore certificate properties file, specify it for the ClassLoader, modify the system property `webservices.soap.custom.crypto.fileName`, and delete the `webservices.soap.permissionHandler.className` system property.

To enable the WS-Security trusted authentication for Oracle WebCenter Discussions, you must:

- Obtain a valid client and server certificate as described in [Section 14.8.4.3, "Setting Up the Keystores"](#).
- Configure WS-Security-related properties on the Discussions server.
- Add the WS-Security-related properties in your Oracle WebCenter Discussions connection created for integrating Discussions and Announcements services into your WebCenter applications.

These configuration steps are described in the following sub-sections:

- [Creating the Keystore Certificate Properties File](#)
- [Specifying the Properties File for ClassLoader](#)
- [Updating the System Properties for WS-Security](#)

### 14.8.2.1 Creating the Keystore Certificate Properties File

The server-side keystore certificate configuration must be stored in a properties file (`keystore.properties`) and specified as a system property on the Discussions server. The properties file then must be loaded in the ClassLoader for the WS-Secure Handler to pick it up.

#### To create the properties file

1. Create a properties file with the following entries:

```
org.apache.ws.security.crypto.provider= <Specify your crypto provider
(typically org.apache.ws.security.components.crypto.Merlin)>
org.apache.ws.security.crypto.merlin.keystore.type=<Specify the keystore type
(either jks or pks)>
org.apache.ws.security.crypto.merlin.keystore.password=<Specify the keystore
password of your server certificate>
org.apache.ws.security.crypto.merlin.keystore.alias=<Specify the keystore alias
of your server certificate>
org.apache.ws.security.crypto.merlin.file=<Specify the absolute path of your
server certificate file. For example, C:\Programs\Discussions\server_public_
certs.keystore>
```

2. Save the file as `keystore.properties`.

### 14.8.2.2 Specifying the Properties File for ClassLoader

There are two ways you can choose either way to specify your `keystore.properties` file based on your setup. This is recommended way when using Clustered Discussions Server installation in Linux to use a same file mounted across different servers.

To specify the properties file for ClassLoader, do one of the following:

- Specify the properties file as the CLASSPATH in `setDomainEnv.sh`.

For Linux:

1. Place the `keystore.properties` file in a directory (for example, `/home/user/keystore/`)
2. Open `MW_HOME/user_projects/domains/wc_domain/bin/setDomainEnv.sh`.
3. Towards the end of the file, add the following lines to specify this directory as the CLASSPATH.

```
if [ "${CLASSPATH}" != "" ] ; then
    CLASSPATH="${CLASSPATH}${CLASSPATHSEP}/home/user/keystore/"
    export CLASSPATH
else
    CLASSPATH="/home/user/keystore/"
    export CLASSPATH
fi
```

Note that the CLASSPATH directory name must end with `"/`.

For Windows:

- a. Place the `keystore.properties` file in a directory (for example, `c:\keystore\`).
- b. Open `MW_HOME\user_projects\domains\wc_domain\bin\setDomainEnv.cmd`.
- c. Towards the end of the file, add the following lines to specify this directory in CLASSPATH.

```
if NOT "%CLASSPATH%"==" (
    set CLASSPATH=%CLASSPATH%;c:\keystore\
) else (
    set CLASSPATH=c:\keystore\
)
```

Note that the CLASSPATH directory name must end with `"\"`.

- Or add the `keystore.properties` file to a `.JAR` file and place the `.JAR` file in your `MW_HOME/user_projects/domains/wc_domain/lib` directory.

### 14.8.2.3 Updating the System Properties for WS-Security

To update your system properties:

1. Log in to the Oracle WebCenter Discussions Admin Console at the following URL:

```
http://host:port/owc_discussions/admin
```

Where `host` and `port` are the address and the port number of the server where you deployed Oracle WebCenter Discussions (for example, `http://localhost:7001/owc_discussions`).

2. Click **System Properties** under **Forum System**. This displays the Jive Properties page.
3. Modify the system property `webservices.soap.custom.crypto.fileName` and specify the properties file that you created (i.e., `keystore.properties`).

Be sure to specify the name of file, and not the directory or `.JAR` name.

4. Under **All Properties**, click the delete icon next to the `webservices.soap.permissionHandler.className` system property.
5. Click **OK**.
6. Extract the `owc_discussions.war` file from `MW_HOME/Oracle_WC1/discussionserver/owc_discussions.ear` or `owc_discussions_sso.ear`, then extract `WEB-INF/classes/jive_extra_startup_content.xml`.
7. Open `WEB-INF/classes/jive_extra_startup_content.xml` and delete or comment out the following entries:

```
<entry name="webservices.soap.permissionHandler.className" overwrite="false"
readonly="false">com.jivesoftware.webcenter.webservices.OraclePermissionHandler
</entry>
```

```
<entry name="webservices.soap.custom.crypto.fileName" overwrite="false"
readonly="false">crypto.properties</entry>
```

8. Save the file.
9. Repackage the `.WAR` file with the updated `WEB-INF/classes/jive_extra_startup_content.xml` file, and then repackage the `.EAR` file with the updated `.WAR` file.
10. Delete the existing installation and install the newly generated `.EAR` file.
11. Restart the `WLS_Services` managed server.

After setting the system properties, your WebCenter application also needs to supply the WS-Security client certificate through the connection settings for Discussion Forum and Announcement Server as described in [Section 11.1, "Setting Up Connections for the Discussions and Announcements Services"](#).

## 14.8.3 Securing Oracle WebLogic Communication Services (OWLCS) with WS-Security

Follow the steps below to configure WS-Security for Oracle WebLogic Communication Services (OWLCS):

1. Provide the **policyURI** when creating the Instant Messaging and Presence (IMP) connection.

When you create the connection to the WS-Security enabled OWLCS server, you must provide the `policyURI`. The value of `policyURI` should be set to `oracle/wss11_saml_token_with_message_protection_client_policy`. If no `policyURI` is supplied, the application will use a non-secure connection. See also [Section 11.2.3, "Registering Instant Messaging and Presence Servers"](#).

2. Supply an alias name for the private key to the IMP connection.

Provide an additional property in the WebCenter IMP connection named `recipient.alias`. Set the value of this property to the alias under which to import the OWLCS certificate. Ensure that this value is unique and is not used already by some other service. If no alias name is supplied, the application uses the default value `webcenter_owlcs`. See also [Section 11-8, "Additional IMP Connection Properties"](#).

3. Determine the private key in the OWLCS keystore (located on the OWLCS instance at `DOMAIN_HOME/config/fmwconfig`).

Use the following command to list the keystore contents:

```
keytool -list -v -keystore Serversidekeystore.jks -storepass password
```

Find the entry with the Entry type set to `keyEntry`. The alias name of this entry is the private key (`orakey` by default).

4. Export the private key from the OWLCS server keystore.

Use the following command to export `orakey` to a certificate file (for example, `orakey.cer`).

```
keytool -exportcert -v -alias orakey -keystore Serversidekeystore.jks
-storepass welcome -rfc -file orakey.cer
```

5. Determine the private key in the WebCenter keystore (on the WebCenter instance at `DOMAIN_HOME/config/fmwconfig`).

If no keystore is found, proceed to step 6. Otherwise, use the following command to list the keystore contents:

```
keytool -list -v -keystore default-keystore.jks -storepass welcome
```

Find the entry with Entry type set to `keyEntry` or `PrivateKeyEntry`. The alias name of this entry is the private key.

If no such entry is found, proceed to step 6. Otherwise, continue at step 7.

6. Generate a private key on WebCenter.

Go to `DOMAIN_HOME/config/fmwconfig` in your WebCenter installation and run the following command to add a key pair to the keystore. The command creates a keystore named `default-keystore.jks` if it doesn't already exist, and adds a new private key entry with alias `orasig` and the password set to `welcome1`. You can optionally change the alias, password and domain name command when you run the command.

```
keytool -genkeypair -keyalg RSA -dname "cn=consumer,dc=example,dc=com"
-alias orasig -keypass welcome1 -keystore default-keystore.jks
-storepass welcome1 -validity 360
```

7. Configure OWLCS on your WebCenter instance to use the private key.

Run the WLST `createCred` command substituting the user and password keys in the first two commands with your private key alias and password.

```
createCred(map='oracle.wsm.security', key='enc-csf-key', user='orasig',
password='welcome1', desc='EncryptionKey')
```

```
createCred(map='oracle.wsm.security', key='sign-csf-key', user='orasig',
password='welcome1', desc='SigningKey')
```

```
createCred(map='oracle.wsm.security', key='keystore-csf-key', user='owsm',
password='welcome1', desc='KeystoreKey')
```

8. Export the private key pair to a certificate.

Export the private key found in step 5 or created in step 6 to a certificate file using the following command:

```
keytool -exportcert -v -alias orasig -keystore default-keystore.jks -storepass
welcome1 -rfc -file orasig.cer
```

9. Import the certificate generated on the OWLCS Server to the WebCenter keystore.

Copy the certificate generated in step 4 to a temporary location on the WebCenter instance. Import the certificate in the WebCenter instance using the alias name from step 2.

Use the following command to import the certificate in the WebCenter keystore:

```
keytool -importcert -alias webcenter_owlcs -file orakey.cer -keystore
default-keystore.jks -storepass welcome1
```

10. Import the WebCenter certificate on the OWLCS instance.

Copy the certificate created in step 8 to a temporary location on the OWLCS instance. Go to `DOMAIN_HOME/config/fmwconfig` and import the certificate in the keystore under a meaningful alias (for example, `webcenter_key`) using the following command:

```
keytool -importcert -alias webcenter_key -file orasig.cer -keystore
Serversidekeystore.jks -storepass welcome
```

## 14.8.4 Securing a WSRP Producer with WS-Security

The following sections describe how to secure access to JSR-168 standards-based WSRP portlets from WebCenter applications:

- [Deploying the Producer](#)
- [Attaching a Policy to the Producer Endpoint](#)
- [Setting Up the Keystores](#)

For a conceptual overview of securing WSRP producers, see "Securing Identity Propagation Through WSRP Producers with WS-Security" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

### 14.8.4.1 Deploying the Producer

Before you configure the producer for WS-Security, you must first deploy your standards-compliant portlet producer to an Oracle WebLogic managed server by performing the steps described in [Section 12.8, "Deploying Portlet Producer Applications"](#).



#### 14.8.4.2 Attaching a Policy to the Producer Endpoint

This section describes how to attach a security policy to a WSRP producer endpoint. The following policies are supported for WSRP producers:

- Username token with password

`wss10_username_token_with_message_protection_service_policy`

This policy enforces message-level protection (message integrity and confidentiality) and authentication for inbound SOAP requests in accordance with the WS-Security 1.0 standard. It uses WS-Security's Basic 128 suite of asymmetric key technologies (specifically, RSA key mechanism for message confidentiality, SHA-1 hashing algorithm for message integrity, and AES-128 bit encryption). The keystore is configured through the security configuration. Authentication is enforced using credentials in the WS-Security UsernameToken SOAP header. The Subject is established against the currently configured identity store.

- Username token without password

`wss10_username_id_propagation_with_msg_protection_service_policy`

This policy enforces message level protection (message integrity and confidentiality) and identity propagation for inbound SOAP requests using mechanisms described by the WS-Security 1.0 standard. Message protection is provided using WS-Security's Basic 128 suite of asymmetric key technologies (specifically, RSA key mechanisms for confidentiality, SHA-1 hashing algorithm for integrity, and AES-128 bit encryption). Identity is set using the user name provided by the UsernameToken WS-Security SOAP header. The Subject is established against the currently configured identity store.

- SAML token

There are two SAML token policies:

- SAML token with message integrity:

`wss10_saml_token_with_message_integrity_service_policy`

This policy provides message-level integrity protection and SAML-based authentication for inbound SOAP requests in accordance with the WS-Security 1.0 standard. It uses WS-Security's Basic 128 suite of asymmetric key technologies, specifically RSA key mechanisms for message confidentiality, and SHA-1 hashing algorithm for message integrity.

- SAML token with message protection:

`wss10_saml_token_with_message_protection_service_policy`

This policy enforces message-level protection and SAML-based authentication for inbound SOAP requests in accordance with the WS-Security 1.0 standard. It uses WS-Security's Basic 128 suite of asymmetric key technologies, specifically RSA key mechanisms for message confidentiality, SHA-1 hashing algorithm for message integrity, and AES-128 bit encryption.

The keystore is configured through the security configuration. It extracts the SAML token from the WS-Security binary security token, and uses those credentials to validate users against the configured identity store.

#### To attach a policy to a producer endpoint

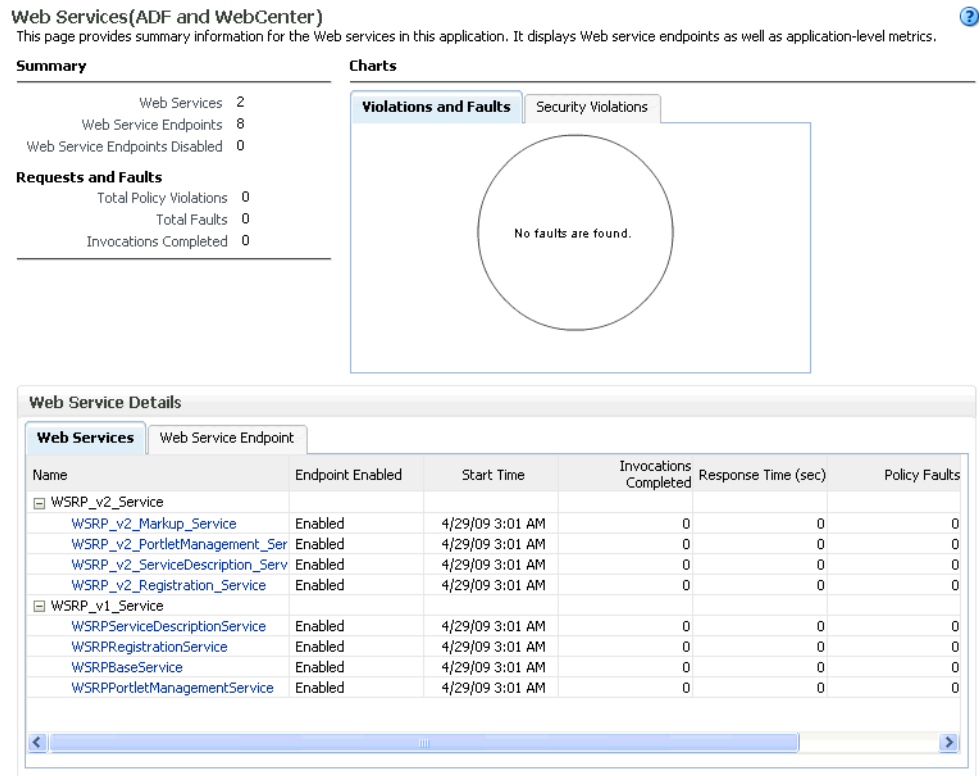
1. Open Fusion Middleware Control and log into the target domain.

For information on logging into Fusion Middleware Control, see [Section 6, "Starting Enterprise Manager Fusion Middleware Control"](#).

2. In the Navigation pane, expand the Application Deployments node, and click the producer to attach a policy to.
3. From the Application Deployment menu, select **Web Services**.

The Web Services Summary page for the producer displays (see [Figure 14–133](#)).

**Figure 14–133 Web Services Summary Page**



This screenshot shows the WebServices Summary page.

\*\*\*\*\*

4. Open the Web Service Endpoint tab and click the endpoint to which to attach a policy.

---

**Note:** Only the markup service ports should be secured (WSRP\_V2\_Markup\_Service and WSRP\_V1\_Markup\_Service).

---

The Web Service Endpoints page for the producer displays (see [Figure 14–134](#)).

**Figure 14–134 Web Service Endpoints Page**

Web Services > Web Service Endpoint

**WSRP\_v2\_Markup\_Service (Web Service Endpoint)** [Web Services Test](#) [Message Log](#) [Diagnostic Log](#)

This page shows details and metrics for the Web service endpoint. The Policies tab lists the policies attached to this Web service endpoint. Attach/Detach takes you to a page where you attach or detach policies. The Configuration tab displays the endpoint configuration.

|                     |          |                      |                        |
|---------------------|----------|----------------------|------------------------|
| Endpoint Enabled    | Enabled  | Transport            | HTTP                   |
| Style               | document | Data Binding         | jaxb20                 |
| SOAP Version        | soap1.1  | Legacy Configuration | False                  |
| Stateful            | False    | Implementation Class | WSRP_v2_Markup_Service |
| Implementation Type | JAX-RPC  | WSDL Document        | WSRP_v2_Markup_Service |

**Operations** Policies Charts Configuration

| Operation Name       | One Way | Action               | Input Encoding | Output Encoding | Invocations Completed | Execution Time Average (ms) |
|----------------------|---------|----------------------|----------------|-----------------|-----------------------|-----------------------------|
| getMarkup            | False   | urn:oasis:names:tc:v | document       | document        | 0                     | 0                           |
| performBlockingInter | False   | urn:oasis:names:tc:v | document       | document        | 0                     | 0                           |
| getResource          | False   | urn:oasis:names:tc:v | document       | document        | 0                     | 0                           |
| initCookie           | False   | urn:oasis:names:tc:v | document       | document        | 0                     | 0                           |
| handleEvents         | False   | urn:oasis:names:tc:v | document       | document        | 0                     | 0                           |
| releaseSessions      | False   | urn:oasis:names:tc:v | document       | document        | 0                     | 0                           |

- Open the Policies tab to display the currently attached policies for the producer (see Figure 14–135).

**Figure 14–135 Web Services Endpoint Policies Page**

Web Services > Web Service Endpoint

**WSRP\_v2\_Markup\_Service (Web Service Endpoint)** [Web Services Test](#) [Message Log](#) [Diagnos](#)

This page shows details and metrics for the Web service endpoint. The Policies tab lists the policies attached to this Web service endpoint. Attach/Detach takes you to a page where you attach or detach policies. The Configuration tab displays the endpoint configuration.

|                     |          |                      |                        |
|---------------------|----------|----------------------|------------------------|
| Endpoint Enabled    | Enabled  | Transport            | HTTP                   |
| Style               | document | Data Binding         | jaxb20                 |
| SOAP Version        | soap1.1  | Legacy Configuration | False                  |
| Stateful            | False    | Implementation Class | WSRP_v2_Markup_Service |
| Implementation Type | JAX-RPC  | WSDL Document        | WSRP_v2_Markup_Service |

**Operations** **Policies** Charts Configuration

[Attach/Detach](#)

| Policy Name | Category | Policy Reference Status | Total Violations | Authentication | Se | Authori |
|-------------|----------|-------------------------|------------------|----------------|----|---------|
| No rows yet |          |                         |                  |                |    |         |

- Click **Attach/Detach** to add or remove a policy. The Attach/Detach Policies page is shown listing the available policies and their descriptions (see Figure 14–136).

**Figure 14–136 Attach/Detach Policies Page**

Web Services > Web Service Endpoint > Attach Policies  
 Attach/Detach Policies(WSRP\_v2\_Markup\_Service) OK Validate

**Attached Policies**

| Name        | Category | Enabled | Description |
|-------------|----------|---------|-------------|
| No rows yet |          |         |             |

▲ Attach ▼ Detach

**Available Policies**

Search  Category  All

| Name  | Category      | Enabled | Description                   |
|---|---------------|---------|-------------------------------|
| oracle/wsaddr_policy  | WS-Addressing | ✓       | This policy causes the pla... |
| oracle/log_policy   | Management    | ✓       | This policy causes the req... |
| oracle/wsmtom_policy  | MTOM Attachn  | ✓       | This Message Transmission ... |
| oracle/binding_authorization_denyall_policy                           | Security      | ✓       | This policy is a special c... |
| oracle/binding_authorization_permitall_policy                         | Security      | ✓       | This policy is a special c... |
| oracle/binding_permission_authorization_policy                        | Security      | ✓       | This policy is a special c... |
| oracle/wss10_message_protection_service_policy                        | Security      | ✓       | This policy enforces messa... |
| oracle/wss10_saml_hok_token_with_message_protection_service_policy    | Security      | ✓       | This policy enforces messa... |
| oracle/wss10_saml_token_service_policy                                | Security      | ✓       | This policy authenticates ... |
| oracle/wss10_saml_token_with_message_integrity_service_policy         | Security      | ✓       | This policy enforces messa... |
| oracle/wss10_saml_token_with_message_protection_service_policy        | Security      | ✓       | This policy enforces messa... |
| oracle/wss10_saml_token_with_message_protection_ski_basic256_service  | Security      | ✓       | This policy enforces messa... |
| oracle/wss10_username_id_propagation_with_msg_protection_service_poll | Security      | ✓       | This policy enforces messa... |

- Under Available Policies, select **Category** and **Security** as the policy category to search, and click the Search icon to list the security policies.
- Select the policies to attach and click **Attach**. Use the **Ctrl** key to select multiple policies.

The policies appear in the list under Attached Policies (see [Figure 14–137](#)).

**Figure 14–137 Attach Detach Policy Page with Policy Attached**

Web Services > Web Service Endpoint > Attach Policies

Attach/Detach Policies(WSRP\_v2\_Markup\_Service) OK Validate Cancel

**Attached Policies**

| Name   | Category | Enabled | Description                   | View Full Description |
|--|----------|---------|-------------------------------|-----------------------|
| oracle/wss10_saml_token_with_message_protection_service_policy | Security | ✓       | This policy enforces messa... | bd                    |

▲ Attach ▼ Detach

**Available Policies**

Search  Security

| Name   | Category | Enabled | Description                   | View Full Description |
|--|----------|---------|-------------------------------|-----------------------|
| oracle/binding_authorization_denyall_policy                          | Security | ✓       | This policy is a special c... | bd                    |
| oracle/binding_authorization_permitall_policy                        | Security | ✓       | This policy is a special c... | bd                    |
| oracle/binding_permission_authorization_policy                       | Security | ✓       | This policy is a special c... | bd                    |
| oracle/wss10_message_protection_service_policy                       | Security | ✓       | This policy enforces messa... | bd                    |
| oracle/wss10_saml_hok_token_with_message_protection_service_policy   | Security | ✓       | This policy enforces messa... | bd                    |
| oracle/wss10_saml_token_service_policy                               | Security | ✓       | This policy authenticates ... | bd                    |
| oracle/wss10_saml_token_with_message_integrity_service_policy        | Security | ✓       | This policy enforces messa... | bd                    |
| oracle/wss10_saml_token_with_message_protection_ski_basic256_service | Security | ✓       | This policy enforces messa... | bd                    |
| oracle/wss10_username_id_propagation_with_msg_protection_service_pol | Security | ✓       | This policy enforces messa... | bd                    |
| oracle/wss10_username_token_with_message_protection_service_policy   | Security | ✓       | This policy enforces messa... | bd                    |
| oracle/wss10_username_token_with_message_protection_ski_basic256_se  | Security | ✓       | This policy enforces messa... | bd                    |
| oracle/wss10_x509_token_with_message_protection_service_policy       | Security | ✓       | This policy enforces messa... | bd                    |
| oracle/wss11_kerberos_token_service_policy                           | Security | ✓       | This policy is enforced in... | bd                    |

This screenshot shows the Attach/Detach Policy page with a policy selected.

\*\*\*\*\*

9. When finished adding polices to attach to the producer endpoint, click **OK**.

#### 14.8.4.3 Setting Up the Keystores

The security credentials of the WSRP producer and WebCenter application can be retrieved and managed using a Java Keystore (JKS). A keystore is a file that provides information about available public and private keys. Keys are used for a variety of purposes, including authentication and data integrity. User certificates and the trust points needed to validate the certificates of peers are also stored securely in the wallet or keystore. See the *Oracle Fusion Middleware Security and Administrator's Guide for Web Services* for information about JKS.

The consumer in the step-by-step procedures below is the WebCenter application, which consumes portlets generated by the remote portlet producer over WSRP. The producer uses the public key of the consumer to verify the authenticity of the security tokens received from the consumer in the WS-Security headers of the requests it receives over its `getMarkup` interface. To do this, the producer needs a Java keystore that contains the certificate of the consumer and the root certificate used to sign it. These certificates are added to the Java keystore as trusted certificates.

This section describes the following tasks:

- [Creating the Keystores](#)
- [Configuring the Keystores](#)
- [Unconfiguring a Keystore Provider](#)

##### 14.8.4.3.1 Creating the Keystores

This section describes how to create keystores and keys using a Java Keystore (JKS). JKS is the proprietary keystore format defined by Sun Microsystems. To create and manage the keys and certificates in the JKS, use the `keytool` utility that is distributed with the Java JDK 6.

To create Java keystores for the consumer and producer:

1. Go to `JDEV_HOME/jdk/bin` and open a command prompt.
2. Using `keytool`, generate a key pair:

```
keytool -genkeypair -keyalg RSA -dname "consumer_dname" -alias consumer_alias  
-keypass key_password  
-keystore keystore -storepass keystore_password -validity days_valid
```

Where:

- `consumer_dname` is the name of the consumer (for example, `cn=consumer,dc=example,dc=com`)
- `consumer_alias` is the alias of the consumer (for example, `consumer`)
- `key_password` is the password for the new public key, (for example, `welcome1`)
- `keystore` is the keystore name, (for example, `consumer.jks`)
- `keystore_password` is the keystore password, (for example, `welcome1`)
- `days_valid` is the number of days for which the key password is valid (for example, `360`).

---

---

**Note:** You must use the `-keyalg` parameter and specify `RSA` as its value as shown above as the default algorithm (`DSA`) used by `keytool` for generating the key is incompatible with Oracle WebServices Security Manager requirements.

---

---

3. Export the public key of the consumer:

```
keytool -exportcert -v -alias consumer_alias -keystore keystore -storepass  
keystore_password -rfc -file certificate_file
```

Where:

- `consumer_alias` is the alias of the consumer (for example, `consumer`)
  - `keystore` is the keystore name, (for example, `consumer.jks`)
  - `keystore_password` is the keystore password, (for example, `welcome1`)
  - `certificate_file` is the file name for the certificate to export the key to (for example, `consumer.cer`)
4. Generate the producer keystore by importing the trusted certificate of consumer:

```
keytool -importcert -alias consumer_alias -file certificate_file -keystore  
keystore -storepass keystore_password
```

Where:

- `consumer_alias` is the alias of the consumer
- `certificate_file` is the certificate file name
- `keystore` is the keystore name

- *keystore\_password* is the keystore password

#### 5. Generate the key pair for the producer:

```
keytool -genkeypair -keyalg RSA -dname "producer_dname" -alias producer_alias
-keypass key_password
-keystore keystore -storepass keystore_password -validity days_valid
```

Where:

- *producer\_dname* is the name of the producer (for example, `cn=producer,dc=example,dc=com`)
- *producer\_alias* is the alias of the producer (for example, `producer`)
- *key\_password* is the password for the new public key, (for example, `welcome1`)
- *keystore* is the keystore name, (for example, `producer.jks`)
- *keystore\_password* is the keystore password, (for example, `welcome1`)
- *days\_valid* is the number of days for which the key password is valid (for example, `1024`)

---

**Note:** You must use the `-keyalg` parameter and specify `RSA` as its value as shown above as the default algorithm (`DSA`) used by `keytool` for generating the key will not work.

---

#### 6. List the contents of the keystore:

```
keytool -list -v -keystore keystore_name -storepass password
```

Where:

- *keystore\_name* is the name of the consumer keystore file (for example, `portal.jks`)
- *password* is the keystore password.

The keystore should now have two key entries.

#### 7. Export the public key of the producer:

```
keytool -exportcert -v -alias producer_alias -keystore keystore -storepass
keystore_password -rfc -file certificate_file
```

Where:

- *producer\_alias* is the alias of the producer (for example, `producer`)
- *keystore* is the keystore name (for example, `producer.jks`)
- *keystore\_password* is the keystore password, (for example, `welcome1`)
- *certificate\_file* is the certificate file name (for example, `producer.cer`)

#### 8. Import the trusted certificate of the producer:

```
keytool -importcert -alias producer_alias -file certificate_file -keystore
keystore_name -storepass keystore_password
```

Where:

- *producer\_alias* is the alias of the producer (for example, `producer`)
- *certificate\_file* is the file name or path for the producer's certificate file (for example, `../producer/producer.cer`)
- *keystore\_name* is the keystore name (for example, `consumer.jks`)
- *keystore\_password* is the keystore password, (for example, `welcome1`)

#### 14.8.4.3.2 Configuring the Keystores

To enable Web Services Security (WS-Security) trusted authentication for the WSRP producer and WebCenter application, you must first configure keystores for both the consumer and producer, and then import the keystore information to the consumer system as described below.

If a keystore provider is already configured, you will first need to unconfigure the existing keystore provider as described in [Section 14.8.4.3.3, "Unconfiguring a Keystore Provider"](#).

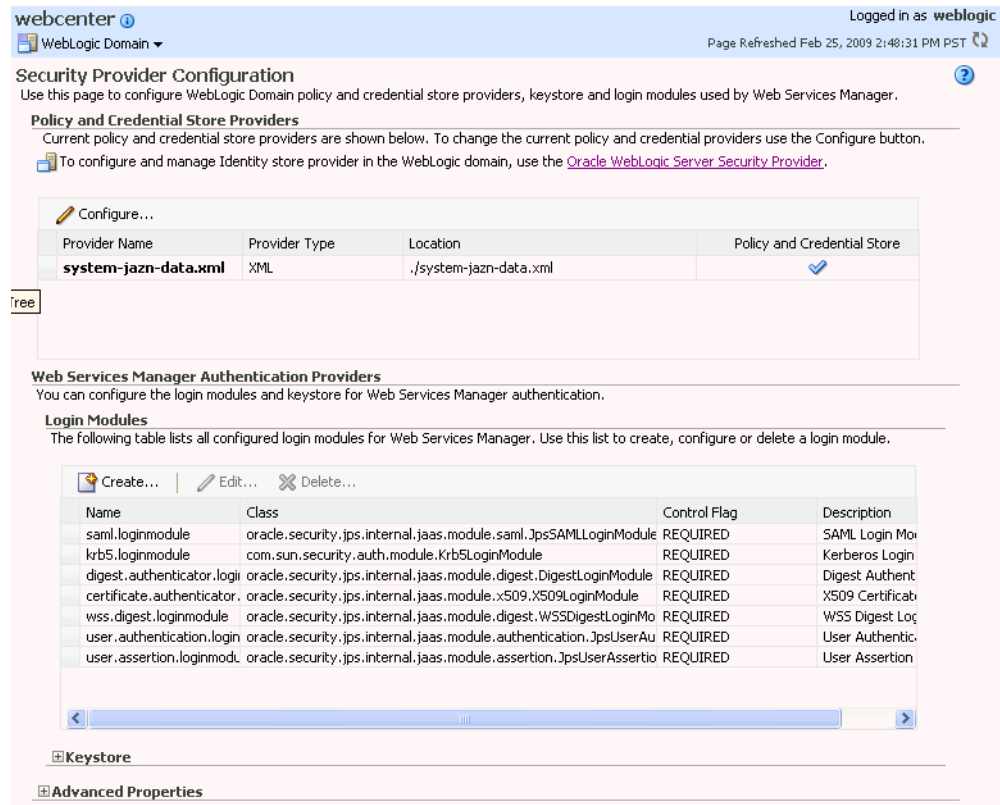
To configure the keystore provider:

1. Copy the corresponding keystores to corresponding servers.
2. Open Fusion Middleware Control and log into the target domain.  
For information on logging into Fusion Middleware Control, see [Section 6, "Starting Enterprise Manager Fusion Middleware Control"](#).
3. In the Navigation pane, expand the WebLogic Domain node and click on the domain (for example, `webcenter`).
4. From the WebLogic Domain menu, select **Security -> Security Provider Configuration**.

The Security Provider Configuration page displays (see [Figure 14-138](#)).

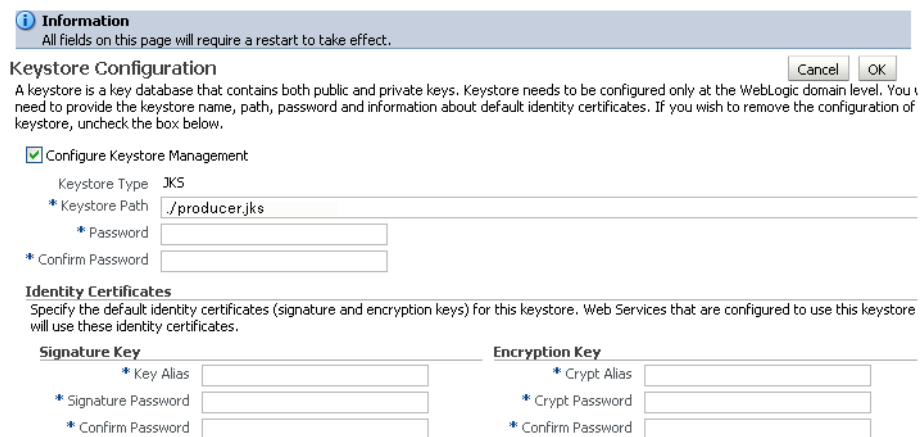


Figure 14–138 Security Provider Configuration Page



5. Expand the Keystore section on the Security Provider Configuration page.
6. Click **Configure**.  
The Keystore Configuration page displays (see Figure 14–139).

Figure 14–139 Keystore Configuration Page



This screenshot shows the Keystore Configuration page.

\*\*\*\*\*

7. Use the **Keystore** section to specify the location of the keystore that contains the certificate and private key that is used for signing some parts (security token and SOAP message body) of the SOAP message, setting the signature key and encryption key parameters, and to set the keystore user name and password.

For detailed parameter information, see [Section 14.8.1.4.2, "Updating the Credential Store in the WebCenter Spaces Instance Using Fusion Middleware Control"](#).

8. Click **OK** to save your settings.
9. Restart the Administration server for the domain.

### 14.8.4.3.3 Unconfiguring a Keystore Provider

If a keystore provider is already configured, you will first need to unconfigure the existing keystore provider before configuring a new provider. To unconfigure, follow the steps below. Otherwise, continue with the steps to configure the producer.

To unconfigure a keystore provider using Fusion Middleware Control:

1. Open Fusion Middleware Control and log into the target domain.
 

For information on logging into Fusion Middleware Control, see [Section 6, "Starting Enterprise Manager Fusion Middleware Control"](#).
2. From the WebLogic Domain menu, select **Security -> Security Provider Configuration**.
 

The Security Provider Configuration page displays (see [Figure 14–138](#)).

**Figure 14–140 Security Provider Configuration Page**

The screenshot displays the 'Security Provider Configuration' page. At the top, it indicates the user is logged in as 'weblogic' and the page was refreshed on Feb 25, 2009. The main heading is 'Security Provider Configuration', with a sub-heading 'Policy and Credential Store Providers'. A table lists the current providers:

| Provider Name        | Provider Type | Location               | Policy and Credential Store         |
|----------------------|---------------|------------------------|-------------------------------------|
| system-jazn-data.xml | XML           | ./system-jazn-data.xml | <input checked="" type="checkbox"/> |

Below this, the 'Web Services Manager Authentication Providers' section is visible, containing a table of login modules:

| Name                       | Class  | Control Flag | Description     |
|----------------------------|--|--------------|-----------------|
| saml.loginmodule           | oracle.security.jps.internal.jaas.module.saml.JpsSAMLLoginModule   | REQUIRED     | SAML Login Mo   |
| krb5.loginmodule           | com.sun.security.auth.module.Krb5LoginModule                       | REQUIRED     | Kerberos Login  |
| digest.authenticator.logii | oracle.security.jps.internal.jaas.module.digest.DigestLoginModule  | REQUIRED     | Digest Authent  |
| certificate.authenticator  | oracle.security.jps.internal.jaas.module.x509.X509LoginModule      | REQUIRED     | X509 Certificab |
| wss.digest.loginmodule     | oracle.security.jps.internal.jaas.module.digest.WSSDigestLoginMo   | REQUIRED     | WSS Digest Loç  |
| user.authentication.login  | oracle.security.jps.internal.jaas.module.authentication.JpsUserAu  | REQUIRED     | User Authentic  |
| user.assertion.loginmod    | oracle.security.jps.internal.jaas.module.assertion.JpsUserAssertio | REQUIRED     | User Assertion  |

3. Expand the Keystore section on the Security Provider Configuration page.
4. Click **Configure**.  
The Keystore Configuration page displays (see [Figure 14–139](#)).

**Figure 14–141 Keystore Configuration Page**

i **Information**  
 All fields on this page will require a restart to take effect.

Cancel OK

**Keystore Configuration**

A keystore is a key database that contains both public and private keys. Keystore needs to be configured only at the WebLogic domain level. You need to provide the keystore name, path, password and information about default identity certificates. If you wish to remove the configuration of keystore, uncheck the box below.

**Configure Keystore Management**

Keystore Type:

\* Keystore Path:

\* Password:

\* Confirm Password:

---

**Identity Certificates**

Specify the default identity certificates (signature and encryption keys) for this keystore. Web Services that are configured to use this keystore will use these identity certificates.

| Signature Key                                  | Encryption Key                               |
|--|--|
| * Key Alias: <input type="text"/>              | * Crypt Alias: <input type="text"/>          |
| * Signature Password: <input type="password"/> | * Crypt Password: <input type="password"/>   |
| * Confirm Password: <input type="password"/>   | * Confirm Password: <input type="password"/> |

5. Uncheck **Configure Keystore Management**.
6. Click **OK**.

## 14.8.5 Securing WebCenter Spaces for Applications Consuming Spaces Client APIs with WS-Security

This section describes how to configure WS-Security for WebCenter Spaces to support custom WebCenter applications that consume WebCenter Spaces client APIs.

This section includes the following subsections:

- [Generating the Keystores](#)
- [Providing the Keystores and Keystore Information to the Application Developer](#)
- [Registering the Keystores](#)
- [Updating the Credential Stores](#)

### 14.8.5.1 Generating the Keystores

Follow the steps below to generate Java keystores for the consumer (the custom WebCenter application) and producer (WebCenter Spaces).

To generate keystores for the consumer and producer:

1. Go to `JDEV_HOME/jdk/bin` and open a command prompt.
2. Using `keytool`, generate a key pair:

```
keytool -genkeypair -keyalg RSA -dname "consumer_dname" -alias consumer_alias
-keypass key_password
-keystore keystore -storepass keystore_password -validity days_valid
```

Where:

- *consumer\_dname* is the name of the consumer (for example, `cn=consumer,dc=example,dc=com`)
- *consumer\_alias* is the alias of the consumer (for example, `consumer`)
- *key\_password* is the password for the new public key, (for example, `welcome1`)
- *keystore* is the keystore name, (for example, `consumer.jks`)
- *keystore\_password* is the keystore password, (for example, `welcome1`)
- *days\_valid* is the number of days for which the key password is valid (for example, `360`).

---

---

**Note:** You must use the `-keyalg` parameter and specify `RSA` as its value as shown above as the default algorithm (DSA) used by `keytool` for generating the key is incompatible with Oracle WebServices Security Manager requirements.

---

---

3. Export the public key for the consumer:

```
keytool -exportcert -v -alias consumer_alias -keystore keystore -storepass keystore_password -rfc -file certificate_file
```

Where:

- *consumer\_alias* is the alias of the consumer (for example, `consumer`)
  - *keystore* is the keystore name, (for example, `consumer.jks`)
  - *keystore\_password* is the keystore password, (for example, `welcome1`)
  - *certificate\_file* is the file name for the certificate to export the key to (for example, `consumer.cer`)
4. Generate the producer keystore by importing the trusted certificate of the consumer:

```
keytool -importcert -alias consumer_alias -file certificate_file -keystore keystore -storepass keystore_password
```

Where:

- *consumer\_alias* is the alias of the consumer
- *certificate\_file* is the certificate file name
- *keystore* is the keystore name
- *keystore\_password* is the keystore password

5. Generate the key pair for the producer:

```
keytool -genkeypair -keyalg RSA -dname "producer_dname" -alias producer_alias -keypass key_password -keystore keystore -storepass keystore_password -validity days_valid
```

Where:

- *producer\_dname* is the name of the producer (for example, `cn=producer,dc=example,dc=com`)
- *producer\_alias* is the alias of the producer (for example, `producer`)

- *key\_password* is the password for the new public key, (for example, `welcome1`)
- *keystore* is the keystore name, (for example, `producer.jks`)
- *keystore\_password* is the keystore password, (for example, `welcome1`)
- *days\_valid* is the number of days for which the key password is valid (for example, `1024`)

---

**Note:** You must use the `-keyalg` parameter and specify `RSA` as its value as shown above as the default algorithm (`DSA`) used by `keytool` for generating the key will not work.

---

**6. List the contents of the keystore:**

```
keytool -list -v -keystore keystore_name -storepass password
```

Where:

- *keystore\_name* is the name of the consumer keystore file (for example, `portal.jks`)
- *password* is the keystore password.

The keystore should now have two key entries.

**7. Export the public key of the producer:**

```
keytool -exportcert -v -alias producer_alias -keystore keystore -storepass keystore_password -rfc -file certificate_file
```

Where:

- *producer\_alias* is the alias of the producer (for example, `producer`)
- *keystore* is the keystore name (for example, `producer.jks`)
- *keystore\_password* is the keystore password, (for example, `welcome1`)
- *certificate\_file* is the certificate file name (for example, `producer.cer`)

**8. Import the trusted certificate of the producer:**

```
keytool -importcert -alias producer_alias -file certificate_file -keystore keystore_name -storepass keystore_password
```

Where:

- *producer\_alias* is the alias of the producer (for example, `producer`)
- *certificate\_file* is the file name or path for the producer's certificate file (for example, `../producer/producer.cer`)
- *keystore\_name* is the keystore name (for example, `consumer.jks`)
- *keystore\_password* is the keystore password, (for example, `welcome1`)

### 14.8.5.2 Providing the Keystores and Keystore Information to the Application Developer

Before registering the keystores, make sure that you have provided the following to the developer creating the application that will be consuming the WebCenter Spaces APIs.

- The consumer keystore to be used to secure the connection. This is a `.jks` file (for example, `consumer.jks`).
- The consumer public alias key stored in the keystore (for example, `consumer`).
- The password of the consumer public alias key (for example, `welcome1`).
- The producer public alias key stored in the consumer keystore (for example, `producer`). This is the alias used when importing the trusted certificate of the producer, and created in step 8 of [Section 14.8.5.1, "Generating the Keystores"](#).
- The consumer keystore password (for example, `welcome1`).

### 14.8.5.3 Registering the Keystores

After you have created the keystores, configure the keystore for WS-Security by performing the following steps. If a keystore provider is already configured, unconfigure the existing keystore provider before proceeding as described in [Section 14.8.4.3.3, "Unconfiguring a Keystore Provider"](#).

To register the keystore provider:

1. Copy the `producer.jks` file to the file system where your producer application is running (for example, `domain_home/config/fmwconfig`).
2. Log into Fusion Middleware Control.  
For information on logging into Fusion Middleware Control, see [Section 6, "Starting Enterprise Manager Fusion Middleware Control"](#).
3. In the Navigation pane, expand the WebLogic Domain node and click on the domain (for example, `webcenter`).
4. From the WebLogic Domain menu, select **Security -> Security Provider Configuration**.

The Security Provider Configuration page displays (see [Figure 14-142](#)).

**Figure 14–142 Security Provider Configuration Page**

webcenter ? WebLogic Domain Logged in as: weblogic  
 Page Refreshed Feb 25, 2009 2:48:31 PM PST ?

### Security Provider Configuration

Use this page to configure WebLogic Domain policy and credential store providers, keystore and login modules used by Web Services Manager.

**Policy and Credential Store Providers**  
 Current policy and credential store providers are shown below. To change the current policy and credential providers use the Configure button.  
 To configure and manage Identity store provider in the WebLogic domain, use the [Oracle WebLogic Server Security Provider](#).

| Provider Name        | Provider Type | Location               | Policy and Credential Store         |
|----------------------|---------------|------------------------|-------------------------------------|
| system-jazn-data.xml | XML           | ./system-jazn-data.xml | <input checked="" type="checkbox"/> |

**Web Services Manager Authentication Providers**  
 You can configure the login modules and keystore for Web Services Manager authentication.

**Login Modules**  
 The following table lists all configured login modules for Web Services Manager. Use this list to create, configure or delete a login module.

| Name                       | Class  | Control Flag | Description      |
|----------------------------|--|--------------|------------------|
| saml.loginmodule           | oracle.security.jps.internal.jaas.module.saml.JpsSAMLLoginModule   | REQUIRED     | SAML Login Mo    |
| krb5.loginmodule           | com.sun.security.auth.module.Krb5LoginModule                       | REQUIRED     | Kerberos Login   |
| digest.authenticator.login | oracle.security.jps.internal.jaas.module.digest.DigestLoginModule  | REQUIRED     | Digest Authent   |
| certificate.authenticator  | oracle.security.jps.internal.jaas.module.x509.X509LoginModule      | REQUIRED     | X509 Certificate |
| wss.digest.loginmodule     | oracle.security.jps.internal.jaas.module.digest.WSSDigestLoginMo   | REQUIRED     | WSS Digest Log   |
| user.authentication.login  | oracle.security.jps.internal.jaas.module.authentication.JpsUserAu  | REQUIRED     | User Authentic   |
| user.assertion.loginmod    | oracle.security.jps.internal.jaas.module.assertion.JpsUserAssertio | REQUIRED     | User Assertion   |

**Keystore**

**Advanced Properties**

- Expand the Keystore section on the Security Provider Configuration page.
- Click **Configure**.  
 The Keystore Configuration page displays (see [Figure 14–143](#)).

**Figure 14–143 Keystore Configuration Page**

**Information**  
 All fields on this page will require a restart to take effect.

**Keystore Configuration** Cancel OK

A keystore is a key database that contains both public and private keys. Keystore needs to be configured only at the WebLogic domain level. You need to provide the keystore name, path, password and information about default identity certificates. If you wish to remove the configuration of keystore, uncheck the box below.

**Configure Keystore Management**

Keystore Type: JKS

\* Keystore Path: /producer.jks

\* Password:

\* Confirm Password:

**Identity Certificates**  
 Specify the default identity certificates (signature and encryption keys) for this keystore. Web Services that are configured to use this keystore will use these identity certificates.

|  |   |
|--|---|
| <p><b>Signature Key</b></p> <p>* Key Alias: <input type="text"/></p> <p>* Signature Password: <input type="text"/></p> <p>* Confirm Password: <input type="text"/></p> | <p><b>Encryption Key</b></p> <p>* Crypt Alias: <input type="text"/></p> <p>* Crypt Password: <input type="text"/></p> <p>* Confirm Password: <input type="text"/></p> |
|--|---|

- In the **Keystore Path** field, specify the location of the keystore that contains the certificate and private key that is used for signing some parts (security token and

- SOAP message body) of the SOAP message, and enter and confirm the keystore **Password**.
8. In the Signature Key section, enter `sign-csf-key` as the **Key Alias**, and enter and confirm the signature key **Password** (the value used for `<key_password>` above) for the new public key, (for example, `welcome1`).
  9. In the Encryption Key section, enter `enc-csf-key` in the **Crypt Key** field, and enter and confirm the encryption key **Password** (the value used for `<key_password>` above) for the new public key, (for example, `welcome1`).
  10. Click **OK** to save your settings.
  11. Restart the WLS Administration server for the domain.

#### 14.8.5.4 Updating the Credential Stores

Follow the steps below to update the credential stores using Fusion Middleware Control, or from the command line using WLST.

##### To update the Credential Store using WLST

Update the credential store using the WLST `createCred` command. Use the following example values to add the `keystore-csf-key`, `enc-csf-key`, and `sign-csf-key` encryption keys. Before running the command, be sure to back up the `cwallet.sso` file.

##### **Example 14–14** *keystore-csf-key*

```
createCred(map="oracle.wsm.security",key="keystore-csf-key",user="keystore-csf-key",password="welcome1",desc="Keystore Password")
```

##### **Example 14–15** *enc-csf-key*

```
createCred(map="oracle.wsm.security",key="enc-csf-key",user="producer",password="welcome1",desc="Enc Password")
```

##### **Example 14–16** *sign-csf-key*

```
createCred(map="oracle.wsm.security",key="sign-csf-key",user="producer",password="welcome1",desc="Enc Password")
```

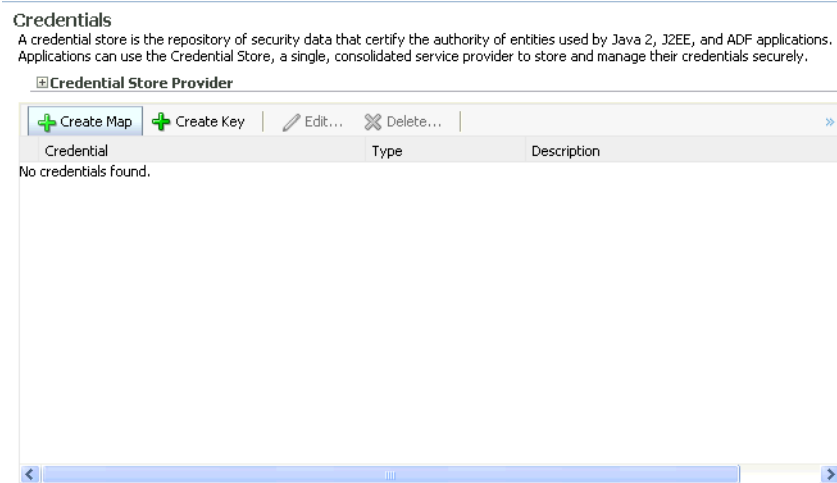
##### To update the Credential Store using Fusion Middleware Control

1. Log into Fusion Middleware Control.
 

For information on logging into Fusion Middleware Control, see [Section 6, "Starting Enterprise Manager Fusion Middleware Control"](#).
2. In the Navigation pane, expand the WebLogic Domain node and click on the domain (for example, `webcenter`).
3. From the WebLogic Domain menu, select **Security -> Credentials**.
 

The Credentials page displays (see [Figure 14–144](#)).



**Figure 14–144 Credentials Page**

4. Click **Create Map**.
5. On the Create Map pop-up, enter `oracle.wsm.security` as the map name and click **OK**.
6. Click **Create Key**.
7. On the Create Key pop-up, select `oracle.wsm.security` as the map, enter `keystore-csf-key` as the **Key**, select `Password` as the **Type**, enter `keystore-csf-key` as the **User Name**, supply the **Password** (in this case, the keystore password of `producer.jks`) from when you created the keystores (for example, `welcome1`), enter an optional description, and click **OK**.
8. Click **Create Key**.
9. On the Create Key pop-up, select `oracle.wsm.security` as the map, enter `sign-csf-key` as the **Key**, select `Password` as the **Type**, enter the public key alias of the keystore used in the custom WebCenter application as the **User Name**, enter the password of the public key used in the custom WebCenter application as the **Password**, enter an optional description, and click **OK**.
10. Click **Create Key**.
11. On the Create Key pop-up, select `oracle.wsm.security` as the map, enter `enc-csf-key` as the **Key**, select `Password` as the **Type**, enter the public key alias of the keystore used in the WebCenter instance (for example, `webcenter`) as the **User Name**, enter the password of the public key used in the custom WebCenter application as the **Password**, enter an optional description, and click **OK**.
12. Restart the Administration server and `WLS_Custom` or managed server on which the custom WebCenter application is hosted.

## 14.9 Securing a PDK-Java Producer

A shared key can be defined for message integrity protection and should be used with SSL. The steps to store a shared key as a password credential are:

- Define a shared key as a password credential in the credential store of the administration server instance. This can be done using either Fusion Middleware Control or WLST.

- Grant the appropriate PDK-Java code access to the credential store (for example, `oracle.portlet-producer.jpdk`).
- Restart the web producer and access the test page. Confirm that the shared key has been picked up correctly by checking the application logs.

---

**Note:** Using a shared key provides only message integrity protection. For complete message protection SSL is required. For more information on securing PDK-Java portlets using SSL, see [Section 14.6.5, "Securing the WebCenter Spaces Connection to Portlet Producers with SSL"](#).

---

## 14.9.1 Defining a Shared Key as a Password Credential

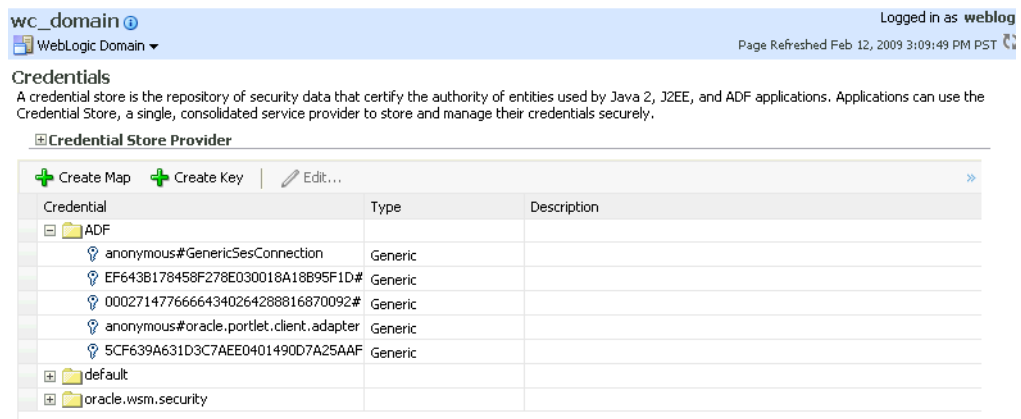
You can define a shared key as a password credential in the credential store of the administration server instance using either Fusion Middleware Control or WLST commands.

### 14.9.1.1 Defining a Shared Key Using Fusion Middleware Control

To define a shared key using Fusion Middleware Control:

1. Log into Fusion Middleware Control.  
For information on logging into Fusion Middleware Control, see [Section 6, "Starting Enterprise Manager Fusion Middleware Control"](#).
2. In the Navigation pane, expand the WebLogic Domain node and click the target domain (for example, `wc_domain`).
3. From the WebLogic Domain menu, select **Security > Credentials**.  
The Credentials pane displays (see [Figure 14-145](#)).

**Figure 14-145 Credentials Pane**



This screenshot shows the Fusion Middleware Control's Credentials pane.

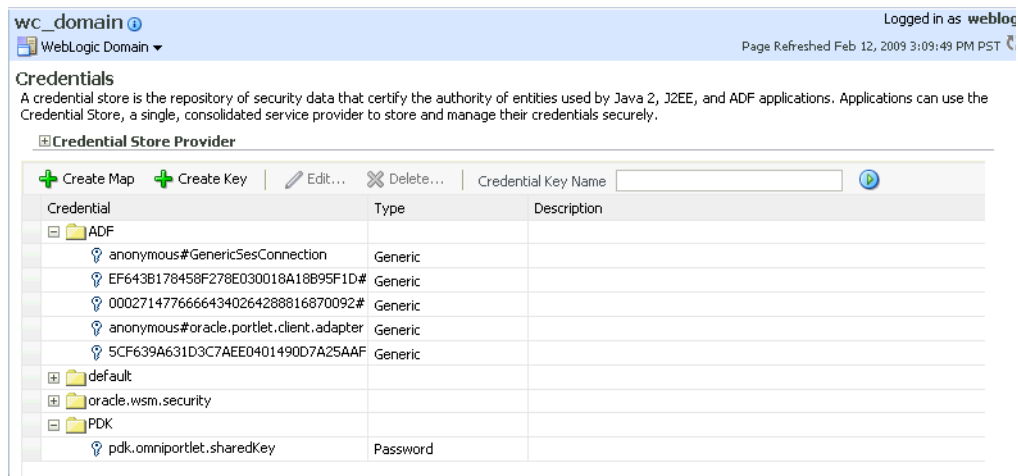
\*\*\*\*\*

4. Click **Create Map** and enter a unique **Map Name** and click **OK**.
5. Click **Create Key** and select the map name of the map you just created.

6. Enter a **User Name** (this value is not used so it could be anything), a **Key** in the form `pdk.<service_id>.<user_name>` (where `<service_id>` is the name of the producer and `<user_name>` is the value you entered for the **User Name**), and a 10 to 20 hexadecimal digit **Password** and click **OK**.

The new key is displayed in the Credential pane (see [Figure 14-146](#)).

**Figure 14-146 Credentials Pane with New Shared Key**



This screenshot shows the Fusion Middleware Control's Credential pane with a newly created shared key.

\*\*\*\*\*

### 14.9.1.2 Defining a Shared Key Using WLST

You can also define a shared key using WLST:

1. Start WLST as described in [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands"](#), and connect to the Administration Server instance for the target domain.
2. Connect to the Administration Server for the target domain with the following command:

```
connect('user_name', 'password', 'host_id:port')
```

Where:

- `user_name` is the name of the user account with which to access the Administration Server (for example, `weblogic`)
- `password` is the password with which to access the Administration Server
- `host_id` is the host ID of the Administration Server
- `port` is the port number of the Administration Server (for example, `7001`).

3. Add a shared key credential for a producer to the credential store using the WLST `createCred` command:

```
createCred(map='MAP', key='MAP.service_id.sharedKey.user_name', user='user_name', password='password')
```

Where:

- *service\_id* is the name of the producer to create the key for (for example, `omniPortlet`)
- *user\_name* is the name of the user. This value is not used so it could be anything.
- *password* is a 10 to 20 hexadecimal digit value.

For example:

```
createCred(map='MAP', key='MAP.omniPortlet.sharedKey', user='sharedKey',
password='1234567890abc')
```

---



---

**Note:** After creating a credential, you can use the WLST `updateCred` command with the same parameters as above to update it.

---



---

#### 4. Restart the producer.

Web producers pick up properties the first time they handle a request (for example, a browser test page request or when they are first registered), so producers should be restarted once a shared key credential has been set up.

## 14.9.2 Granting the PDK-Java Code Access to the Credential Store

After defining the shared key, the next step is to give the Web producer code (a shared library) read access to the credential store (defined as a permission class). The codebase URL for the shared library used for most Web producers will look like:

```
file:${domain.home}/servers/WLS_Portlet/tmp/_WL_
user/oracle.portlet-producer.jpdk/-
```

which grants access to any file under the shared library directory. There are exceptions to this where the Web producer doesn't use the usual shared library. The Tools Web producer, for example, packages its code differently due to classloading considerations. The URL in this case would look like this:

```
file:${domain.home}/servers/WLS_Portlet/tmp/_WL_user/portalTools_11.1.1.1.0/-
```

The permission class is:

```
oracle.security.jps.service.credstore.CredentialAccessPermission
```

There are two ways to give a shared library access to the credentials:

- [Granting Access Using Fusion Middleware Control](#)
- [Granting Access Using WLST](#)

### 14.9.2.1 Granting Access Using Fusion Middleware Control

Follow the steps below to add a grant where the Web producer code is granted access to the credential store, an existing grant is copied, and the codebase URL is changed to a Web producer code base URL.

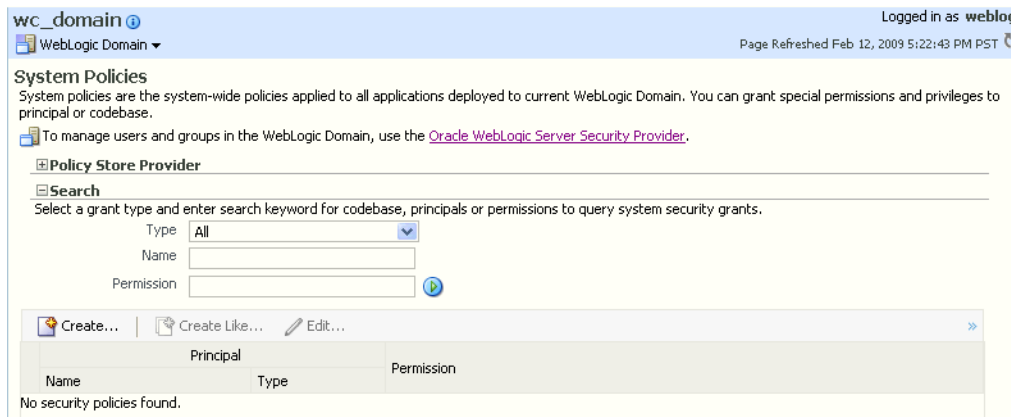
To add a grant using Fusion Middleware Control:

#### 1. Log into Fusion Middleware Control.

For information on logging into Fusion Middleware Control, see [Section 6, "Starting Enterprise Manager Fusion Middleware Control"](#).

2. In the Navigation pane, expand the WebLogic Domain node and click the target domain (for example, `wc_domain`).
3. From the WebLogic Domain menu, select **Security > System Policies**.  
The System Policies pane displays (see [Figure 14-147](#)).

**Figure 14-147 System Policies Pane**



4. Click **Create**.  
The Create System Grant pane displays (see [Figure 14-148](#)).

**Figure 14-148 Create System Grant Pane**



5. In the **Grant To** combo box, select Codebase.
6. In the Codebase field, enter the URL of the PDK shared library that accesses the credential store.
7. Under Permissions, click **Add**.  
The Add Permissions pane displays (see [Figure 14-149](#)).

**Figure 14–149 Add Permission Pane**

**Add Permission**

Select from permissions and resources used in system policies of this domain. Enter search criteria to search for right permissions.

**Search**

Type:

Name:

Permission:

Search Results

| Name                        | Type | Permission |
|-----------------------------|------|------------|
| No security policies found. |      |            |

Customize resource or actions for selected permission.

**Customize**

Name:

Resource Name:

OK Cancel

8. Do a search for all codebases, select one that has the needed permission class and click **OK**.
9. Now update it with the required details.
10. Display the test page in a browser (thereby making a request to the Web producer which will pick up the shared key). Then check the log.

#### 14.9.2.2 Granting Access Using WLST

To define a shared key using WLST:

1. Start WLST as described in [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands"](#).
2. Connect to the Administration Server for the target domain with the following command:

```
connect('user_name','password','host_id:port')
```

Where:

- *user\_name* is the name of the user account with which to access the Administration Server (for example, weblogic)
  - *password* is the password with which to access the Administration Server
  - *host\_id* is the host ID of the Administration Server
  - *port* is the port number of the Administration Server (for example, 7001).
3. Define a shared key using the `grantPermission` command:

```
grantPermission(appStripe=None,principalClass=None,principalName=None,
codeBaseURL='Codebase',
permClass='Class',permTarget='context=SYSTEM,
mapName=PDK,keyName='*',permActions='read')
```

Where:

- *Codebase* is the codebase URL
- *Class* is the permissions class  
(`oracle.security.jps.service.credstore.CredentialAccessPermission`)

For example:

```
grantPermission(appStripe=None,principalClass=None,principalName=None,codeBaseURL='file:${domain.home}/servers/WLS_Portlet/tmp/_WL_user/-',permClass='oracle.security.jps.service.credstore.CredentialAccessPermission',permTarget='context=SYSTEM,mapName=PDK,keyName=*',permActions='read')
```





---

## Monitoring Oracle WebCenter Performance

Oracle Enterprise Manager Fusion Middleware Control Console provides a Web-based user interface for monitoring the real-time performance of WebCenter applications, including any producers and portlets that WebCenter applications may use.

Performance monitoring helps administrators identify issues and performance bottlenecks in their environment. This chapter describes the range of performance metrics available for WebCenter applications and how to monitor them through Fusion Middleware Control. It also describes how to troubleshoot issues by analyzing information that is recorded in WebCenter diagnostic log files.

Administrators who monitor WebCenter applications regularly, will learn to recognize trends as they develop and prevent performance problems in the future.

This chapter includes the following sections:

- [Understanding WebCenter Performance Metrics](#)
- [Viewing Performance Information](#)
- [Viewing and Configuring Log Information](#)

### **Audience**

The content of this chapter is intended for Fusion Middleware administrators (users granted the `Admin`, `Operator`, or `Monitor` role through the Oracle WebLogic Server Administration Console). See also, [Section 1.8, "Understanding Administrative Operations, Roles, and Tools"](#).

## 15.1 Understanding WebCenter Performance Metrics

Through Fusion Middleware Control, administrators can monitor the performance and availability of all the components and services that make up WebCenter applications, as well as the application as a whole.

To make best use of the information displayed it is important that you understand how performance metrics are calculated and what they mean. All WebCenter's performance metrics are listed and described here for your reference. Some applications (such as WebCenter Spaces) might utilize the full range of social networking, personal productivity, and collaboration service metrics listed, while others may only utilize one or two of these services.

This section includes the following subsections:

- [Overview of Metric Collection: Recent History and Since Startup](#)
- [Overview of Common Metrics](#)

- [Common Performance Issues and Actions](#)
- [Overview of Service-Specific Metrics](#)
- [Service-Specific Performance Issues and Actions](#)
- [Group Space Metrics](#)

### 15.1.1 Overview of Metric Collection: Recent History and Since Startup

Performance metrics are automatically enabled for Oracle WebCenter. In other words, you do not need to set options or perform any extra configuration to collect performance metrics. If you encounter a problem, such as, an application running slowly or hanging, you can view particular metrics to find out more information about the problem as Fusion Middleware Control provides real-time data.

The following types of metrics are available for Oracle WebCenter:

#### Since Startup

At any given time, real-time metrics are available for the duration for which the WebLogic Server hosting WebCenter applications was up and running. The real-time metrics that are collected or aggregated since the startup of the container are displayed for WebCenter as **Since Startup**. These metrics provide data aggregated over the life time of the WebLogic Server. The aggregated data enables you to understand overall system performance and compare the performance of recent requests shown in **Recent History**.

---

---

**Note:** Metric collection starts afresh after the container is restarted. Data collected prior to the restart becomes unavailable.

---

---

#### Recent History

In addition to the **Since Startup** metrics, Oracle WebCenter metrics are also configured to capture the performance data every five minutes. This metric data is used in conjunction with the Since Startup metrics and is made available as **Recent History** metrics.

All metrics seen under Recent History are calculated using just the recent metrics. For example, if a service is used for a short time, but it is not accessed at all for the last 15 minutes, then the Since Startup metrics for the service shows numbers greater than 0, whilst the Recent History metrics for that service are all zero. The Recent History metrics enable you to assess real-time performance of a live site based on data collected just from recent runtime access.

Typically, Recent History shows data for the recent 10-15 minutes. However, there are scenarios when the data is not for the last 10-15 minutes:

- If the WebLogic Server has just been started up, and has been running for less than 10-15 minutes, then Recent History shows data for the duration for which the server has been up and running.
- Metric collection stops temporarily if no metric requests are detected over a long period of time. The collection restarts when the client next requests metrics. If metric collection stops, then Recent History initially shows data for the period since metric collection stopped. As soon as the metric collection starts again, the data starts displaying metrics for the recent 10-15 minutes.

While diagnosing a live site, navigate to the WebCenter metric pages and see the **Services Summary** section to identify services that are actively used and/or are taking

longer than expected. Click the **Refresh** icon next to the time stamp to refresh metrics with live data. Then, click the particular service and repeat these steps to determine which specific operation in the service is taking long. If needed, navigate to application pages that use the service and set the application to trigger the runtime metrics to get more data.

## 15.1.2 Overview of Common Metrics

Fusion Middleware Control provides capabilities to monitor performance of WebCenter Web 2.0 Services in the following ways:

- Services summary: Summary of performance metrics for each service used in a WebCenter application. [Table 15–1](#) lists services that use common performance metrics. [Table 15–2](#) describes service metrics.
- Most popular operations and response time for individual service operations. [Table 15–3](#) describes these metrics.
- Per operation metrics: Performance metrics for individual service operations. [Table 15–1](#) lists common performance metrics used to monitor performance of individual operations. [Table 15–3](#) describes these metrics.

**Table 15–1 Common Performance Metrics**

| Service           | Service Summary<br>(Since Startup and Recent History)   | Per Operation Metrics<br>(Since Startup and Recent History)   |
|-------------------|---|---|
| Announcements     | The performance metrics include: <ul style="list-style-type: none"> <li>■ Status</li> <li>■ Successful Invocations (%)</li> <li>■ Invocations</li> <li>■ Average Time (ms)</li> </ul> | The performance metrics include: <ul style="list-style-type: none"> <li>■ Most Popular Operations</li> <li>■ Response Time</li> <li>■ Invocations</li> <li>■ Average Time (ms)</li> <li>■ Maximum Time (ms)<br/>(Since Startup only)</li> </ul>                                       |
| BPEL Worklist     | The performance metrics include: <ul style="list-style-type: none"> <li>■ Status</li> <li>■ Successful Invocations (%)</li> <li>■ Invocations</li> <li>■ Average Time (ms)</li> </ul> | Not applicable  |
| Discussion Forums | The performance metrics include: <ul style="list-style-type: none"> <li>■ Status</li> <li>■ Successful Invocations (%)</li> <li>■ Invocations</li> <li>■ Average Time (ms)</li> </ul> | The performance metrics include: <ul style="list-style-type: none"> <li>■ Most Popular Operations</li> <li>■ Response Time</li> <li>■ Successful Invocations (%)</li> <li>■ Invocations</li> <li>■ Average Time (ms)</li> <li>■ Maximum Time (ms)<br/>(Since Startup only)</li> </ul> |

**Table 15–1 (Cont.) Common Performance Metrics**

| <b>Service</b>                       | <b>Service Summary<br/>(Since Startup and Recent History)</b>   | <b>Per Operation Metrics<br/>(Since Startup and Recent History)</b>   |
|--------------------------------------|---|---|
| External Applications                | The performance metrics include: <ul style="list-style-type: none"> <li>■ Status</li> <li>■ Successful Invocations (%)</li> <li>■ Invocations</li> <li>■ Average Time (ms)</li> </ul> | The performance metrics include: <ul style="list-style-type: none"> <li>■ Most Popular Operations</li> <li>■ Response Time</li> <li>■ Successful Invocations (%)</li> <li>■ Invocations</li> <li>■ Average Time (ms)</li> <li>■ Maximum Time (ms) (Since Startup only)</li> </ul> |
| Group Space Events                   | The performance metrics include: <ul style="list-style-type: none"> <li>■ Status</li> <li>■ Successful Invocations (%)</li> <li>■ Invocations</li> <li>■ Average Time (ms)</li> </ul> | The performance metrics include: <ul style="list-style-type: none"> <li>■ Most Popular Operations</li> <li>■ Response Time</li> <li>■ Successful Invocations (%)</li> <li>■ Invocations</li> <li>■ Average Time (ms)</li> <li>■ Maximum Time (ms) (Since Startup only)</li> </ul> |
| Import/Export                        | The performance metrics include: <ul style="list-style-type: none"> <li>■ Status</li> <li>■ Successful Invocations (%)</li> <li>■ Invocations</li> <li>■ Average Time (ms)</li> </ul> | The performance metrics include: <ul style="list-style-type: none"> <li>■ Most Popular Operations</li> <li>■ Response Time</li> <li>■ Successful Invocations (%)</li> <li>■ Invocations</li> <li>■ Average Time (ms)</li> <li>■ Maximum Time (ms) (Since Startup only)</li> </ul> |
| Instant Messaging and Presence (IMP) | The performance metrics include: <ul style="list-style-type: none"> <li>■ Status</li> <li>■ Successful Invocations (%)</li> <li>■ Invocations</li> <li>■ Average Time (ms)</li> </ul> | The performance metrics include: <ul style="list-style-type: none"> <li>■ Most Popular Operations</li> <li>■ Response Time</li> <li>■ Successful Invocations (%)</li> <li>■ Invocations</li> <li>■ Average Time (ms)</li> <li>■ Maximum Time (ms) (Since Startup only)</li> </ul> |

**Table 15–1 (Cont.) Common Performance Metrics**

| <b>Service</b> | <b>Service Summary<br/>(Since Startup and Recent History)</b>  | <b>Per Operation Metrics<br/>(Since Startup and Recent History)</b>  |
|----------------|--|--|
| Lists          | <p>The performance metrics include:</p> <ul style="list-style-type: none"> <li>■ Status</li> <li>■ Successful Invocations (%)</li> <li>■ Invocations</li> <li>■ Average Time (ms)</li> </ul> | <p>The performance metrics include:</p> <ul style="list-style-type: none"> <li>■ Most Popular Operations</li> <li>■ Response Time</li> <li>■ Successful Invocations (%)</li> <li>■ Invocations</li> <li>■ Average Time (ms)</li> <li>■ Maximum Time (ms) (Since Startup only)</li> </ul> |
| Mail           | <p>The performance metrics include:</p> <ul style="list-style-type: none"> <li>■ Status</li> <li>■ Successful Invocations (%)</li> <li>■ Invocations</li> <li>■ Average Time (ms)</li> </ul> | <p>The performance metrics include:</p> <ul style="list-style-type: none"> <li>■ Most Popular Operations</li> <li>■ Response Time</li> <li>■ Successful Invocations (%)</li> <li>■ Invocations</li> <li>■ Average Time (ms)</li> <li>■ Maximum Time (ms) (Since Startup only)</li> </ul> |
| Notes          | <p>The performance metrics include:</p> <ul style="list-style-type: none"> <li>■ Status</li> <li>■ Successful Invocations (%)</li> <li>■ Invocations</li> <li>■ Average Time (ms)</li> </ul> | <p>The performance metrics include:</p> <ul style="list-style-type: none"> <li>■ Most Popular Operations</li> <li>■ Response Time</li> <li>■ Successful Invocations (%)</li> <li>■ Invocations</li> <li>■ Average Time (ms)</li> <li>■ Maximum Time (ms) (Since Startup only)</li> </ul> |
| Pages          | <p>The performance metrics include:</p> <ul style="list-style-type: none"> <li>■ Status</li> <li>■ Successful Invocations (%)</li> <li>■ Invocations</li> <li>■ Average Time (ms)</li> </ul> | <p>The performance metrics include:</p> <ul style="list-style-type: none"> <li>■ Most Popular Operations</li> <li>■ Response Time</li> <li>■ Successful Invocations (%)</li> <li>■ Invocations</li> <li>■ Average Time (ms)</li> <li>■ Maximum Time (ms) (Since Startup only)</li> </ul> |

**Table 15–1 (Cont.) Common Performance Metrics**

| <b>Service</b>  | <b>Service Summary<br/>(Since Startup and Recent History)</b>   | <b>Per Operation Metrics<br/>(Since Startup and Recent History)</b>   |
|-----------------|---|---|
| Recent Activity | The performance metrics include: <ul style="list-style-type: none"> <li>▪ Status</li> <li>▪ Successful Invocations (%)</li> <li>▪ Invocations</li> <li>▪ Average Time (ms)</li> </ul> | Not available   |
| RSS News Feed   | The performance metrics include: <ul style="list-style-type: none"> <li>▪ Status</li> <li>▪ Successful Invocations (%)</li> <li>▪ Invocations</li> <li>▪ Average Time (ms)</li> </ul> | Not available   |
| Search          | The performance metrics include: <ul style="list-style-type: none"> <li>▪ Status</li> <li>▪ Successful Invocations (%)</li> <li>▪ Invocations</li> <li>▪ Average Time (ms)</li> </ul> | The performance metrics include: <ul style="list-style-type: none"> <li>▪ Most Popular Operations</li> <li>▪ Response Time</li> <li>▪ Successful Invocations (%)</li> <li>▪ Invocations</li> <li>▪ Average Time (ms)</li> <li>▪ Maximum Time (ms) (Since Startup only)</li> </ul> |

Table 15–2 describes metrics used for monitoring performance of all operations.

**Table 15–2 Description of Common Metrics - Summary (All Operations)**

| <b>Metric</b>              | <b>Description</b>   |
|----------------------------|--|
| Status                     | The current status of the service: <ul style="list-style-type: none"> <li>▪ <b>Up</b> (Green Up Arrow) - Indicates that a service is up and running and the last operation was successful.</li> <li>▪ <b>Down</b> (Red Down Arrow) - Indicates that a service is not currently available. The last operation was unsuccessful due to an unexpected error or exception. User errors, such as an authentication failure, do not change the status to Down.</li> <li>▪ <b>Unknown</b> (Clock) - Indicates that a service is unable to query the status of the WebCenter application for some reason.</li> </ul> |
| Successful Invocations (%) | Percentage of a service invocations that succeeded. Successful Invocations (%) is equal to the number of successful invocations divided by the invocation count: <ul style="list-style-type: none"> <li>- Since Startup</li> <li>- Recent History</li> </ul> If Successful Invocations (%) is below 100%, check the diagnostic logs to establish why service requests are failing. See, <a href="#">Section 15.3, "Viewing and Configuring Log Information"</a> .  |

**Table 15–2 (Cont.) Description of Common Metrics - Summary (All Operations)**

| <b>Metric</b>     | <b>Description</b>   |
|-------------------|--|
| Invocations       | <p>This metric shows number of service invocations per minute:</p> <ul style="list-style-type: none"> <li>- Since Startup</li> <li>- Recent History</li> </ul> <p>This metric provides data on how frequently a particular service is being invoked for processing of operations. Comparing this metric across services can help determine the most frequently used Web 2.0 Services in the application.</p> |
| Average Time (ms) | <p>The average time taken to process operations associated with a service. This metric can be used in conjunction with the Invocations metric to assess the total time spent in processing service operations.</p> <ul style="list-style-type: none"> <li>- Since Startup</li> <li>- Recent History</li> </ul>   |

[Table 15–3](#) describes metrics used to monitor performance of each operation performed by a service or component.

**Table 15–3 Description of Common Metrics - Per Operation**

| <b>Metric</b>           | <b>Description</b>   |
|-------------------------|--|
| Most Popular Operations | <p>The number of invocations per operation (displayed on a chart).</p> <p>The highest value on the chart indicates which operation is used the most.</p> <p>The lowest value indicates which operation is used the least.</p>  |
| Response Time           | <p>The average time to process operations associated with a service since the WebCenter application started up (displayed on a chart).</p> <p>The highest value on the chart indicates the worst performing operation.</p> <p>The lowest value indicates which operation is performing the best.</p>   |
| Operation               | <p>The operation being monitored. See also, <a href="#">Section 15.1.4, "Overview of Service-Specific Metrics"</a>.</p>  |
| Invocations             | <p>The number of invocations, per operation:</p> <ul style="list-style-type: none"> <li>- Since Startup</li> <li>- Recent History</li> </ul> <p>This metric provides data on how frequently a particular service is being invoked for processing of operations. Comparing this metric across services can help determine the most frequently used Web 2.0 Services in the application.</p> |
| Average Time (ms)       | <p>The average time taken to process each operation:</p> <ul style="list-style-type: none"> <li>- Since Startup</li> <li>- Recent History</li> </ul>   |
| Maximum Time (ms)       | <p>The maximum time taken to process each operation.</p>   |

### 15.1.3 Common Performance Issues and Actions

This section provides information on identifying generic performance-related issues.

If a metric is out-of-bound, do the following:

- Check system resources, such as memory, CPU, network, external processes, or other factors.
- Check other metrics to see if the problem is system-wide or only in a particular service.
- If the issue is related to a particular service, then check if the back-end server is down or overloaded.
- If the WebLogic Server has been running for an elongated duration, compare the **Since Startup** metrics with the **Recent History** metrics to determine if performance has recently deteriorated, and if so, by how much.
- Verify connection configuration information associated with the service to see if it is incorrect or no longer valid. See also, [Appendix A, "WebCenter Configuration."](#)
- When the status of a service is Down or some operations do not work, then validate, test, and ping the back-end server through direct URLs, as described in [Chapter 11, "Managing Services."](#)

If a service is reconfigured, but the container is not restarted to uptake the changes, then the service becomes unavailable.

#### 15.1.4 Overview of Service-Specific Metrics

This section describes per operation metrics for all services and components. This section includes the following sub sections:

- [Announcements Metrics](#)
- [BPEL Worklist Metrics](#)
- [Content Repository \(Documents Service\) Metrics](#)
- [Discussions Metrics](#)
- [External Application Metrics](#)
- [Group Space Events Metrics](#)
- [Instant Messaging and Presence \(IMP\) Metrics](#)
- [Import and Export Metrics](#)
- [List Metrics](#)
- [Mail Metrics](#)
- [Note Metrics](#)
- [Page Metrics](#)
- [Portlet Producer Metrics](#)
- [Portlet Metrics](#)
- [RSS News Feed Metrics](#)
- [Recent Activity Metrics](#)
- [Search Metrics](#)

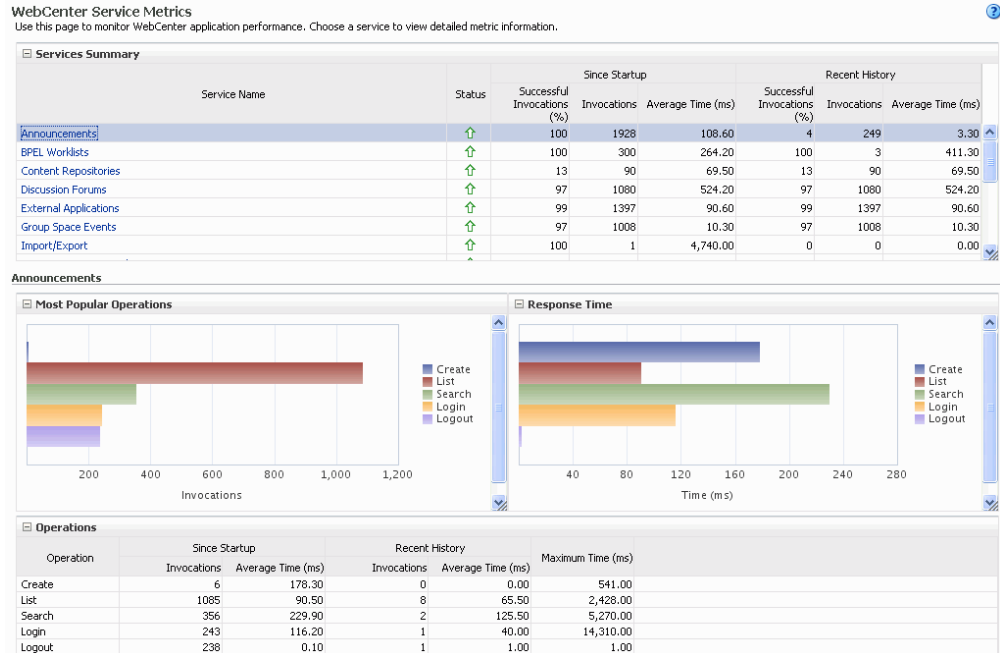
To access live performance metrics for your WebCenter application, see [Section 15.2, "Viewing Performance Information."](#)



### 15.1.4.1 Announcements Metrics

Performance metrics associated with the Announcements service (Figure 15–1) are described in Table 15–4 and Section 15.1.2, "Overview of Common Metrics."

**Figure 15–1** *Announcement Metrics*



To monitor these metrics through Fusion Middleware Control, see Section 15.2, "Viewing Performance Information."

**Table 15–4** *Announcements Service - Operations Monitored*

| Operation | Description  | Performance Issues - User Action  |
|-----------|--|---|
| Login     | Logs a WebCenter user (accessing the Announcements service) into the discussions server that is hosting announcements. | For service-specific causes, see Section 15.1.5.1, "Announcements Service."<br>For common causes, see Section 15.1.3, "Common Performance Issues and Actions."  |
| Logout    | Logs a WebCenter user out of the discussions server that is hosting announcements.                                     | For service-specific causes, see Section 15.1.5.1, "Announcements Service."<br>For common causes, see Section 15.1.3, "Common Performance Issues and Actions."  |
| Search    | Searches for terms within announcement text.   | If Announcement searches are failing, verify that Announcement text contains the search terms.<br>For other causes, see Section 15.1.5.1, "Announcements Service."<br>For common causes, see Section 15.1.3, "Common Performance Issues and Actions." |

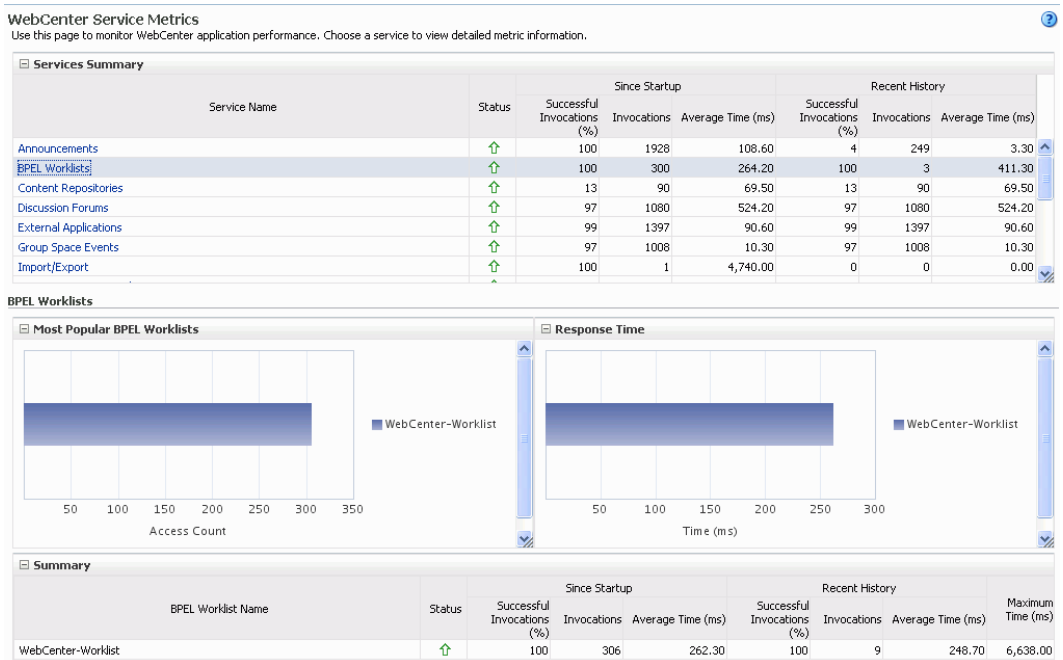
**Table 15–4 (Cont.) Announcements Service - Operations Monitored**

| Operation | Description                        | Performance Issues - User Action   |
|-----------|------------------------------------|--|
| Create    | Creates an announcement.           | For service-specific causes, see <a href="#">Section 15.1.5.1, "Announcements Service."</a><br><br>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a> |
| List      | Retrieves a list of announcements. | For service-specific causes, see <a href="#">Section 15.1.5.1, "Announcements Service."</a><br><br>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a> |

### 15.1.4.2 BPEL Worklist Metrics

Performance metrics associated with the BPEL Worklist service ([Figure 15–2](#)) are described in [Section 15.1.2, "Overview of Common Metrics."](#)

**Figure 15–2 BPEL Worklist Metrics**



To monitor these metrics through Fusion Middleware Control, see [Section 15.2, "Viewing Performance Information."](#)

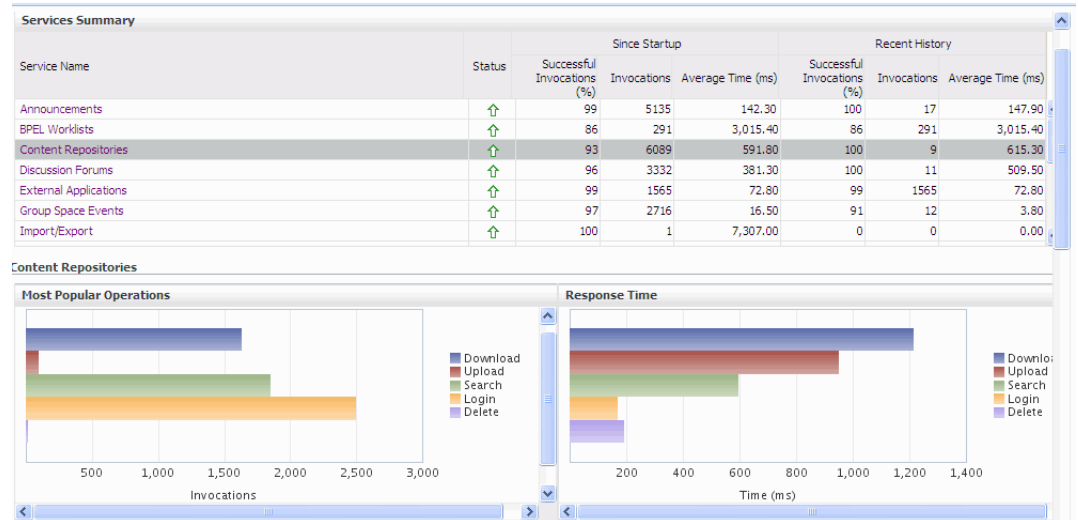
### 15.1.4.3 Content Repository (Documents Service) Metrics

Performance metrics associated with the Documents service ([Figure 15–3](#) and [Figure 15–4](#)) are described in the following tables:

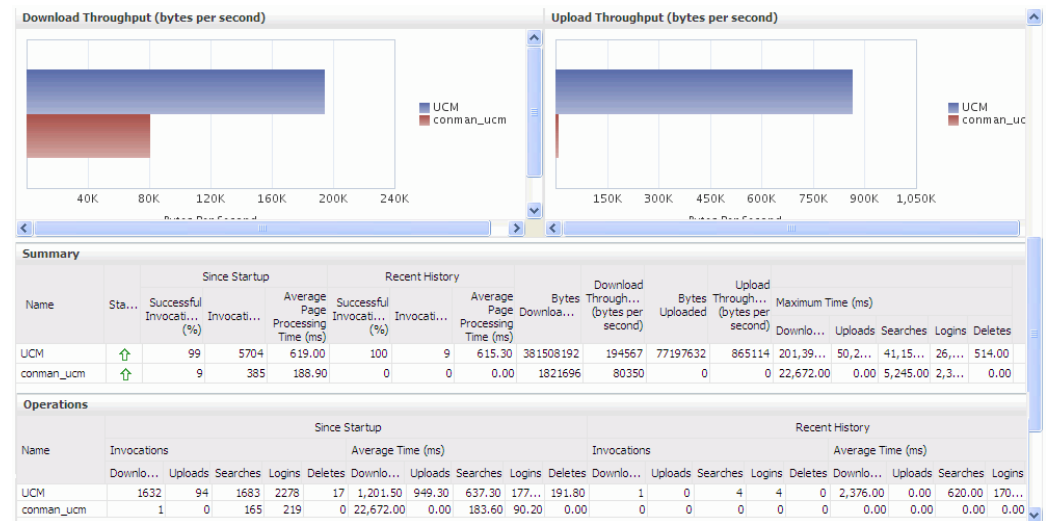
- [Table 15–5, "Documents Service - Operations Monitored"](#)
- [Table 15–6, "Content Repository Metrics - Summary \(All Repositories\)"](#)
- [Table 15–7, "Content Repository Metrics - Operation Summary Per Repository"](#)

■ Table 15–8, "Content Repository Metrics - Operation Detail Per Repository"

**Figure 15–3 Content Repository Metrics**



**Figure 15–4 Content Repository Metrics - Per Operation**



To monitor these metrics through Fusion Middleware Control, see [Section 15.2, "Viewing Performance Information."](#)

**Table 15–5 Documents Service - Operations Monitored**

| Operation | Description  | Performance Issues - User Action   |
|-----------|--|--|
| Download  | Downloads one or more documents from a content repository. | <p>For service-specific causes, see <a href="#">Section 15.1.5.3, "Content Repository (Documents) Service."</a></p> <p>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a></p> |

**Table 15–5 (Cont.) Documents Service - Operations Monitored**

| Operation | Description  | Performance Issues - User Action  |
|-----------|--|---|
| Upload    | Uploads one or more documents to a content repository.                         | For service-specific causes, see <a href="#">Section 15.1.5.3, "Content Repository (Documents) Service."</a><br><br>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a> |
| Search    | Searches for documents stored in a content repository.                         | For service-specific causes, see <a href="#">Section 15.1.5.3, "Content Repository (Documents) Service."</a><br><br>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a> |
| Login     | Establishes a connection to the content repository and authenticates the user. | For service-specific causes, see <a href="#">Section 15.1.5.3, "Content Repository (Documents) Service."</a><br><br>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a> |
| Delete    | Deletes one or more documents stored in a content repository.                  | For service-specific causes, see <a href="#">Section 15.1.5.3, "Content Repository (Documents) Service."</a><br><br>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a> |

**Table 15–6 Content Repository Metrics - Summary (All Repositories)**

| Metric | Description   |
|--------|---|
| Status | <p>The current status of the Documents service:</p> <ul style="list-style-type: none"> <li>■ <b>Up</b> (Green Up Arrow) - Indicates that the Documents service is up and running and the last operation was successful.</li> <li>■ <b>Down</b> (Red Down Arrow) - Indicates that the Documents service is not currently available or service requests are failing. This also indicates that the last operation was unsuccessful due to an unexpected error or exception. User errors, such as an authentication failure, do not change the status to <b>Down</b>.</li> </ul> <p>If you are having problems with the Documents service, check the diagnostic logs to establish why this service is "Down". See, <a href="#">Section 15.3, "Viewing and Configuring Log Information."</a></p> <p>Some typical causes of failure include:</p> <ul style="list-style-type: none"> <li>- Content repository is down or not responding.</li> <li>- Network connectivity issues exist between the application and one or more content repositories.</li> <li>- Connection configuration information associated with one or more content repositories is incorrect or no longer valid.</li> </ul> <ul style="list-style-type: none"> <li>■ <b>Clock</b> - Unable to query the status of the service for some reason.</li> </ul> |

**Table 15–6 (Cont.) Content Repository Metrics - Summary (All Repositories)**

| <b>Metric</b>                          | <b>Description</b>  |
|--|---|
| Successful Invocations (%)             | <p>The percentage of Documents service invocations that succeeded (Upload, Download, Search Login, Delete):</p> <ul style="list-style-type: none"> <li>- Since Startup</li> <li>- Recent History</li> </ul> <p>If Successful Invocations (%) is below 100%, check the diagnostic logs to establish why service requests are failing. See, <a href="#">Section 15.3, "Viewing and Configuring Log Information."</a></p>                            |
| Invocations                            | <p>The number of Documents service invocations per minute (Upload, Download, Search Login, Delete):</p> <ul style="list-style-type: none"> <li>- Since Startup</li> <li>- Recent History</li> </ul> <p>This metric provides data on how frequently a particular service is being invoked for processing of operations. Comparing this metric across services can help determine the most frequently used Web 2.0 Services in the application.</p> |
| Average Time (ms)                      | <p>The average time taken to process operations associated with the Documents service (Upload, Download, Search Login, Delete):</p> <ul style="list-style-type: none"> <li>- Since Startup</li> <li>- Recent History</li> </ul>   |
| Most Popular Operations                | <p>The number of invocations per operation (displayed on a chart).</p> <p>The highest value on the chart indicates which operation is used the most.</p> <p>The lowest value indicates which operations is used the least.</p>  |
| Response Time                          | <p>The average time to process operations associated with the Documents service since the WebCenter application started up (displayed on a chart).</p> <p>The highest value on the chart indicates the worst performing operation.</p> <p>The lowest value indicates which operations is performing the best.</p>   |
| Download Throughput (bytes per second) | The rate at which the Documents service downloads documents.  |
| Upload Throughput (bytes per second)   | The rate at which the Documents service uploads documents   |

**Table 15–7 Content Repository Metrics - Operation Summary Per Repository**

| Metric                                 | Description   |
|--|---|
| Status                                 | <p>The current status of the content repository:</p> <ul style="list-style-type: none"> <li>■ <b>Up</b> (Green Up Arrow) - Indicates that the content repository is up and running and the last operation was successful.</li> <li>■ <b>Down</b> (Red Down Arrow) - Indicates that the content repository is not currently available or service requests are failing. It also indicates that the last operation was unsuccessful due to an unexpected error or exception. User errors, such as an authentication failure, do not change the status to <b>Down</b>.</li> </ul> <p>If you are having problems with a content repository, check the diagnostic logs to establish why this service is "Down". See, <a href="#">Section 15.3, "Viewing and Configuring Log Information."</a></p> <p>Some typical causes of failure include:</p> <ul style="list-style-type: none"> <li>- Content repository is down or not responding.</li> <li>- Network connectivity issues exist between the application and one or more content repositories.</li> <li>- Connection configuration information associated with one or more content repositories is incorrect or no longer valid.</li> </ul> <ul style="list-style-type: none"> <li>■ <b>Clock</b> - Unable to query the status of the service for some reason.</li> </ul> |
| Successful Invocations (%)             | <p>The percentage of Documents service invocations that succeeded (Upload, Download, Search, Login, Delete) for this content repository:</p> <ul style="list-style-type: none"> <li>- Since Startup</li> <li>- Recent History</li> </ul> <p>If Successful Invocations (%) is below 100%, check the diagnostic logs to establish why service requests are failing. See, <a href="#">Section 15.3, "Viewing and Configuring Log Information"</a>.</p>   |
| Invocations                            | <p>The number of Documents service invocations per minute (Upload, Download, Search, Login, Delete) for this content repository:</p> <ul style="list-style-type: none"> <li>- Since Startup</li> <li>- Recent History</li> </ul> <p>This metric provides data on how frequently a particular service is being invoked for processing of operations. Comparing this metric across services can help determine the most frequently used Web 2.0 Services in the application.</p>  |
| Average Page Processing Time (ms)      | <p>The average time taken to process operations associated with the Documents service (Upload, Download, Search, Login, Delete) for this content repository:</p> <ul style="list-style-type: none"> <li>- Since Startup</li> <li>- Recent History</li> </ul>  |
| Bytes Downloaded                       | <p>The volume of data that the Documents service has downloaded from this content repository.</p>   |
| Download Throughput (bytes per second) | <p>The rate at which the Documents service downloads documents from this content repository.</p>  |
| Bytes Uploaded                         | <p>The volume of data that the Documents service has uploaded from this content repository.</p>   |

**Table 15–7 (Cont.) Content Repository Metrics - Operation Summary Per Repository**

| Metric                               | Description   |
|--------------------------------------|---|
| Upload Throughput (bytes per second) | The rate at which the Documents service uploads documents from this content repository.   |
| Maximum Time (ms)                    | The maximum time to process operations associated with the Documents service (Upload, Download, Search, Login, Delete) for this content repository. |

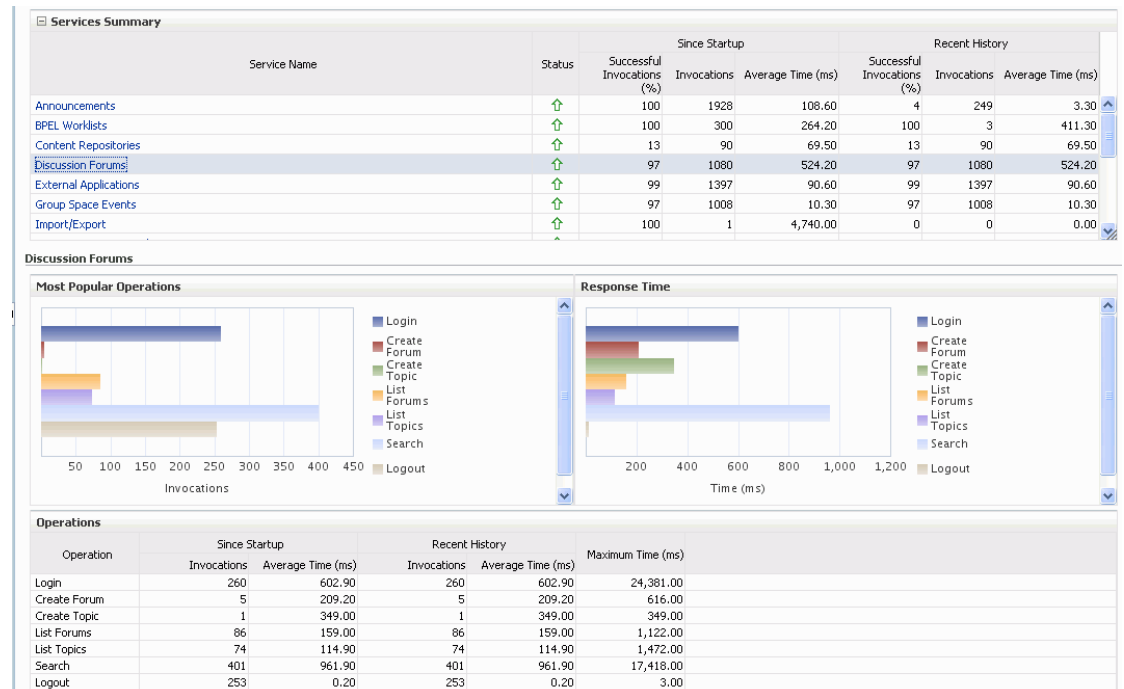
**Table 15–8 Content Repository Metrics - Operation Detail Per Repository**

| Metric                       | Description   |
|------------------------------|---|
| Invocations                  | <p>The number of Documents service invocations per operation (Upload, Download, Search, Login, Delete):</p> <ul style="list-style-type: none"> <li>- Since Startup</li> <li>- Recent History</li> </ul> <p>This metric provides data on how frequently a particular service is being invoked for processing of operations. Comparing this metric across services can help determine the most frequently used Web 2.0 Services in the application.</p> |
| Average Processing Time (ms) | <p>The average time taken to process each operation associated with the Documents service (Upload, Download, Search, Login, Delete):</p> <ul style="list-style-type: none"> <li>- Since Startup</li> <li>- Recent History</li> </ul>  |

**15.1.4.4 Discussions Metrics**

Performance metrics associated with the Discussions service (Figure 15–5) are described in Table 15–9 and Section 15.1.2, "Overview of Common Metrics."

**Figure 15–5 Discussion Metrics**



To monitor these metrics through Fusion Middleware Control, see [Section 15.2, "Viewing Performance Information."](#)

**Table 15–9 Discussions Service - Operations Monitored**

| Operation    | Description   | Performance Issues - User Action   |
|--------------|---|--|
| Login        | Logs a WebCenter user (accessing the Discussions service) into the discussions server that is hosting discussions forums. | <p>For service-specific causes, see <a href="#">Section 15.1.5.4, "Discussions Service."</a></p> <p>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a></p>  |
| Logout       | Logs a WebCenter user out of the discussions server that is hosting discussion forums.                                    | <p>For service-specific causes, see <a href="#">Section 15.1.5.4, "Discussions Service."</a></p> <p>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a></p>  |
| Create Forum | Creates a discussion forum in the discussions server, under a specific category.  | <p>If you are having problems creating forums, it may be due to:</p> <ul style="list-style-type: none"> <li>■ Category under which the discussion forum needs to be created has been deleted.</li> <li>■ User does not have permissions to create discussion forums.</li> </ul> <p>For other service-specific causes, see <a href="#">Section 15.1.5.4, "Discussions Service."</a></p> <p>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a></p>  |
| Create Topic | Creates a topic in the discussions server, under a specific forum.  | <p>If you are having problems creating forums, it may be due to:</p> <ul style="list-style-type: none"> <li>■ Discussion forum under which the topic needs to be created has been deleted.</li> <li>■ User does not have permissions to create topics.</li> </ul> <p>For other service-specific causes, see <a href="#">Section 15.1.5.4, "Discussions Service."</a></p> <p>For information on common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a></p> |



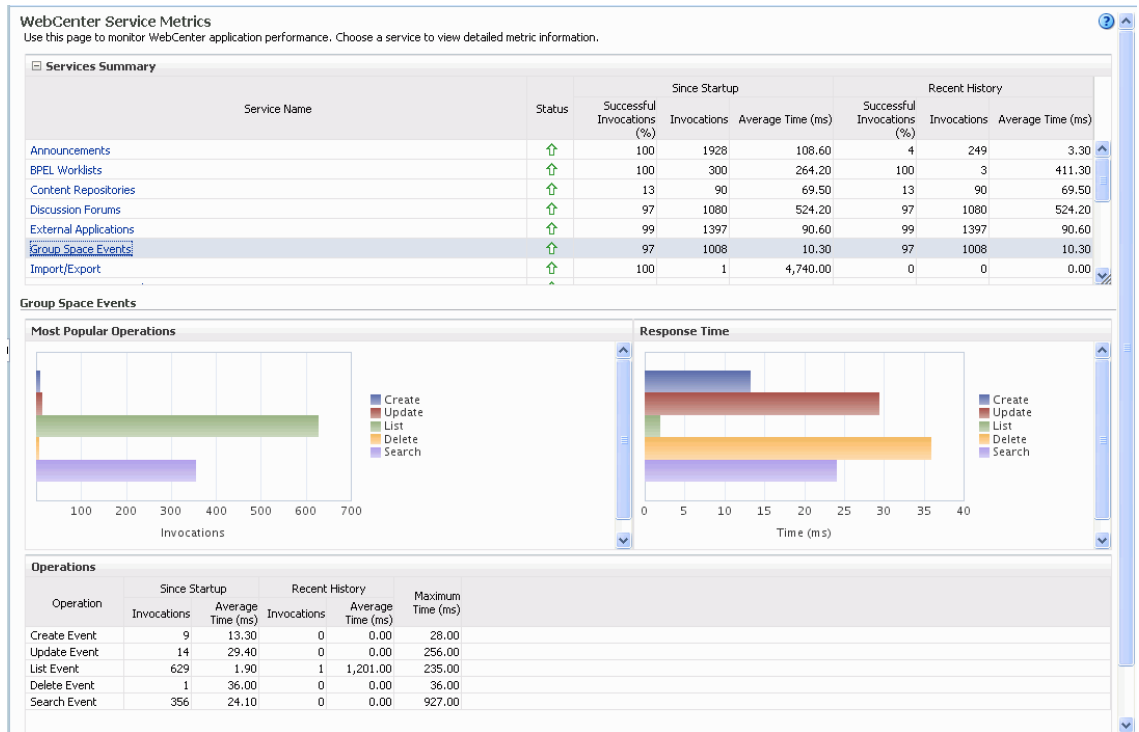
**Table 15–9 (Cont.) Discussions Service - Operations Monitored**

| Operation   | Description  | Performance Issues - User Action  |
|-------------|--|---|
| List Forums | Retrieves a list of forums, under a specific category, from the discussion server. | <p>If you are having problems creating forums, it may be due to:</p> <ul style="list-style-type: none"> <li>■ User does not have permissions to view forums in the category.</li> <li>■ Category from which to fetch forums has been deleted.</li> </ul> <p>For other service-specific causes, see <a href="#">Section 15.1.5.4, "Discussions Service."</a></p> <p>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a></p>                |
| List Topics | Retrieves a list of topics, under a specific forum, from the discussion server.    | <p>If you are having problems creating forums, it may be due to:</p> <ul style="list-style-type: none"> <li>■ User does not have permissions to view topics in the forum.</li> <li>■ Forum from which to fetch topics has been deleted.</li> </ul> <p>For other service-specific causes, see <a href="#">Section 15.1.5.4, "Discussions Service."</a></p> <p>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a></p>                      |
| Search      | Searches for terms within discussion forum text, in the discussions server.        | <p>If you are having problems creating forums, it may be due to:</p> <ul style="list-style-type: none"> <li>■ No topic/messages exist with the specified search term.</li> <li>■ Category or forum in which the search term object resides has been deleted.</li> </ul> <p>For other service-specific causes, see <a href="#">Section 15.1.5.4, "Discussions Service."</a></p> <p>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a></p> |

#### 15.1.4.5 Group Space Events Metrics

Performance metrics associated with the group space Events service are described in [Table 15–10](#) and [Section 15.1.2, "Overview of Common Metrics."](#)

**Figure 15–6 Group Space Events Metrics**



To monitor these metrics through Fusion Middleware Control, see [Section 15.2, "Viewing Performance Information."](#)

**Table 15–10 Events Service - Operations Monitored**

| Operation    | Description   | Performance Issues - User Action  |
|--------------|---|---|
| Create Event | Creates a group space event in the WebCenter repository.        | For service-specific causes, see <a href="#">Section 15.1.5.6, "Group Space Events Service."</a><br><br>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a> |
| Update Event | Updates a group space event stored in the WebCenter repository. | For service-specific causes, see <a href="#">Section 15.1.5.6, "Group Space Events Service."</a><br><br>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a> |
| Delete Event | Deletes a group space event in the WebCenter repository.        | For service-specific causes, see <a href="#">Section 15.1.5.6, "Group Space Events Service."</a><br><br>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a> |
| List Event   | Retrieves a list of events from the WebCenter repository.       | For service-specific causes, see <a href="#">Section 15.1.5.6, "Group Space Events Service."</a><br><br>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a> |

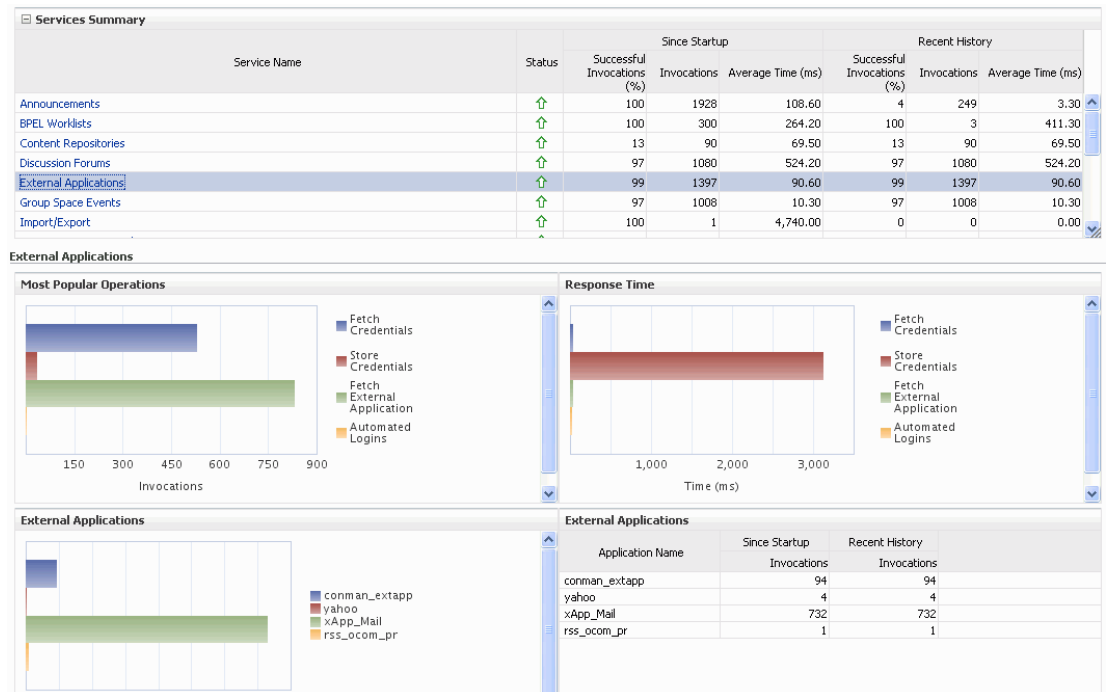
**Table 15–10 (Cont.) Events Service - Operations Monitored**

| Operation    | Description                           | Performance Issues - User Action  |
|--------------|---------------------------------------|---|
| Search Event | Searches for terms within event text. | For service-specific causes, see <a href="#">Section 15.1.5.6, "Group Space Events Service."</a><br><br>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a> |

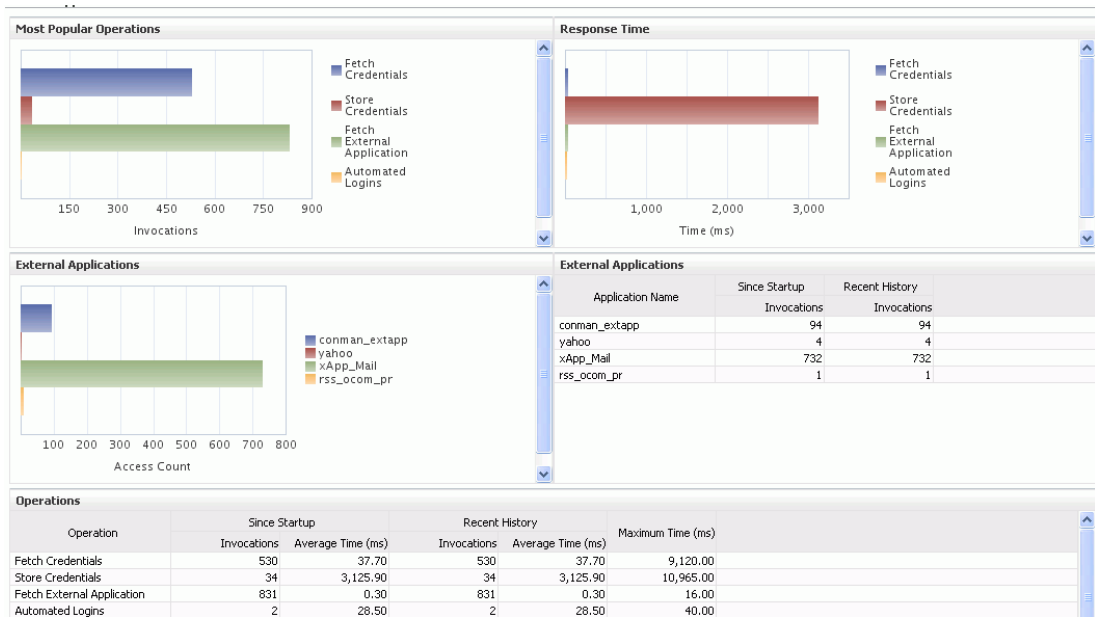
### 15.1.4.6 External Application Metrics

Performance metrics associated with the External Application service are described in [Table 15–11](#) and [Section 15.1.2, "Overview of Common Metrics."](#)

**Figure 15–7 External Application Metrics**



**Figure 15–8 External Application Metrics - Per Operation**



To monitor these metrics through Fusion Middleware Control, see [Section 15.2, "Viewing Performance Information."](#)

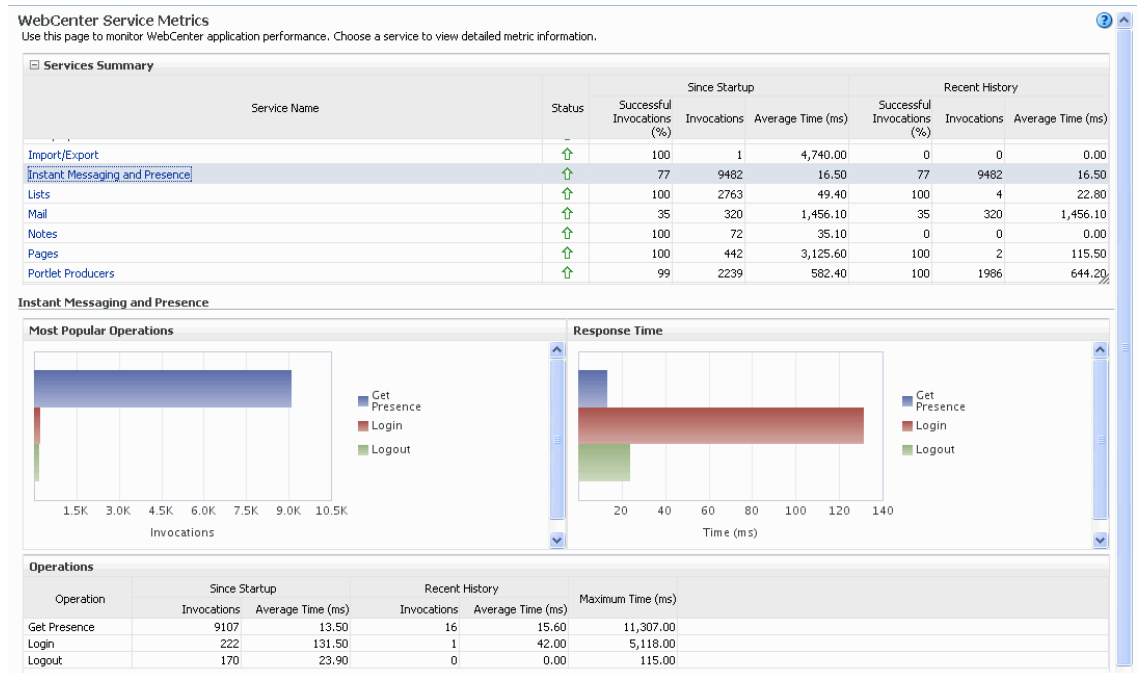
**Table 15–11 External Applications - Operations Monitored**

| Operation                  | Description  | Performance Issues - User Action   |
|----------------------------|--|--|
| Fetch Credentials          | Retrieves credentials for an external application.                                       | For service-specific causes, see <a href="#">Section 15.1.5.5, "External Applications Service."</a><br><br>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a> |
| Store Credentials          | Stores user credentials for an external application.                                     | For service-specific causes, see <a href="#">Section 15.1.5.5, "External Applications Service."</a><br><br>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a> |
| Fetch External Application | Retrieves an external application.   | For service-specific causes, see <a href="#">Section 15.1.5.5, "External Applications Service."</a><br><br>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a> |
| Automated Logins           | Logs a WebCenter user in to an external application (using the automated login feature). | For service-specific causes, see <a href="#">Section 15.1.5.5, "External Applications Service."</a><br><br>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a> |

### 15.1.4.7 Instant Messaging and Presence (IMP) Metrics

Performance metrics associated with the Instant Messaging and Presence (IMP) service (Figure 15–9) are described in Table 15–12 and Section 15.1.2, "Overview of Common Metrics."

**Figure 15–9 IMP Metrics**



To monitor these metrics through Fusion Middleware Control, see Section 15.2, "Viewing Performance Information."

**Table 15–12 Instant Messaging and Presence Service - Operations Monitored**

| Operation    | Description  | Performance Issues - User Action  |
|--------------|--|---|
| Get Presence | Retrieves user presence information from the IMP server.                 | For service-specific causes, see Section 15.1.5.7, "Instant Messaging and Presence (IMP) Service."<br><br>For common causes, see Section 15.1.3, "Common Performance Issues and Actions." |
| Login        | Logs a WebCenter user (accessing the IMP service) into the IMP server.   | For service-specific causes, see Section 15.1.5.7, "Instant Messaging and Presence (IMP) Service."<br><br>For common causes, see Section 15.1.3, "Common Performance Issues and Actions." |
| Logout       | Logs a WebCenter user (accessing the IMP service) out of the IMP server. | For service-specific causes, see Section 15.1.5.7, "Instant Messaging and Presence (IMP) Service."<br><br>For common causes, see Section 15.1.3, "Common Performance Issues and Actions." |

### 15.1.4.8 Import and Export Metrics

Performance metrics associated with import and export services (Figure 15–10) are described in Table 15–13 and Section 15.1.2, "Overview of Common Metrics." These metrics apply to WebCenter Spaces only.

**Figure 15–10 Import/Export Metrics**

**WebCenter Service Metrics**  
Use this page to monitor WebCenter application performance. Choose a service to view detailed metric information.

| Service Name          | Status | Since Startup              |             |                   | Recent History             |             |                   |
|-----------------------|--------|----------------------------|-------------|-------------------|----------------------------|-------------|-------------------|
|                       |        | Successful Invocations (%) | Invocations | Average Time (ms) | Successful Invocations (%) | Invocations | Average Time (ms) |
| Announcements         | ↑      | 100                        | 1928        | 108.60            | 4                          | 249         | 3.30              |
| BPEL Worklists        | ↑      | 100                        | 300         | 264.20            | 100                        | 3           | 411.30            |
| Content Repositories  | ↑      | 13                         | 90          | 69.50             | 13                         | 90          | 69.50             |
| Discussion Forums     | ↑      | 97                         | 1080        | 524.20            | 97                         | 1080        | 524.20            |
| External Applications | ↑      | 99                         | 1397        | 90.60             | 99                         | 1397        | 90.60             |
| Group Space Events    | ↑      | 97                         | 1008        | 10.30             | 97                         | 1008        | 10.30             |
| Import/Export         | ↑      | 100                        | 1           | 4,740.00          | 0                          | 0           | 0.00              |

| Operations | Since Startup              |             |                   | Recent History             |             |                   | Maximum Time (ms) |
|------------|----------------------------|-------------|-------------------|----------------------------|-------------|-------------------|-------------------|
|            | Successful Invocations (%) | Invocations | Average Time (ms) | Successful Invocations (%) | Invocations | Average Time (ms) |                   |
| Import     | 100                        | 1           | 4,740.00          | 0                          | 0           | 0.00              | 4,740.00          |

To monitor these metrics through Fusion Middleware Control, see Section 15.2, "Viewing Performance Information."

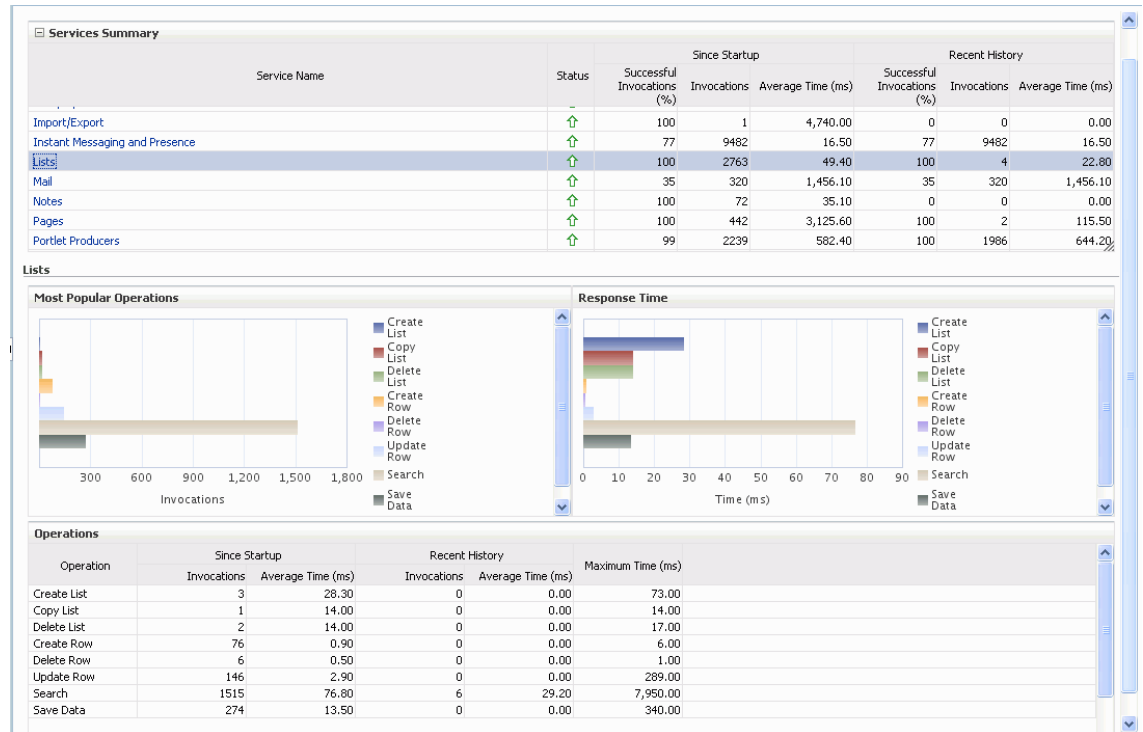
**Table 15–13 Import/Export - Operations Monitored**

| Operation | Description                              | Performance Issues - User Action   |
|-----------|--|--|
| Export    | Exports an entire WebCenter application. | For service-specific causes, see Section 15.1.5.8, "Import and Export."<br><br>For common causes, see Section 15.1.3, "Common Performance Issues and Actions." |
| Import    | Imports entire WebCenter application.    | For service-specific causes, see Section 15.1.5.8, "Import and Export."<br><br>For common causes, see Section 15.1.3, "Common Performance Issues and Actions." |

### 15.1.4.9 List Metrics

(WebCenter Spaces only) Performance metrics associated with the List service (Figure 15–11) are described in Table 15–14 and Section 15.1.2, "Overview of Common Metrics."

Figure 15–11 List Metrics



To monitor these metrics through Fusion Middleware Control, see [Section 15.2, "Viewing Performance Information."](#)

Table 15–14 List service - Operations Monitored

| Operation   | Description   | Performance Issues - User Action  |
|-------------|---|---|
| Create List | Creates a list in the user session.   | For service-specific causes, see <a href="#">Section 15.1.5.9, "Lists Service."</a>             |
|             | The Save Data operation commits new lists to the MDS repository.  | For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a> |
| Copy List   | Copies a list and its data in the user session.   | For service-specific causes, see <a href="#">Section 15.1.5.9, "Lists Service."</a>             |
|             | The Save Data operation commits copied lists and list data to the MDS repository and the WebCenter repository (the database where list data is stored). | For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a> |
| Delete List | Deletes a list and its data in the user session.  | For service-specific causes, see <a href="#">Section 15.1.5.9, "Lists Service."</a>             |
|             | The Save Data operation commits list changes to the MDS repository and the WebCenter repository (the database where list data is stored).               | For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a> |

**Table 15–14 (Cont.) List service - Operations Monitored**

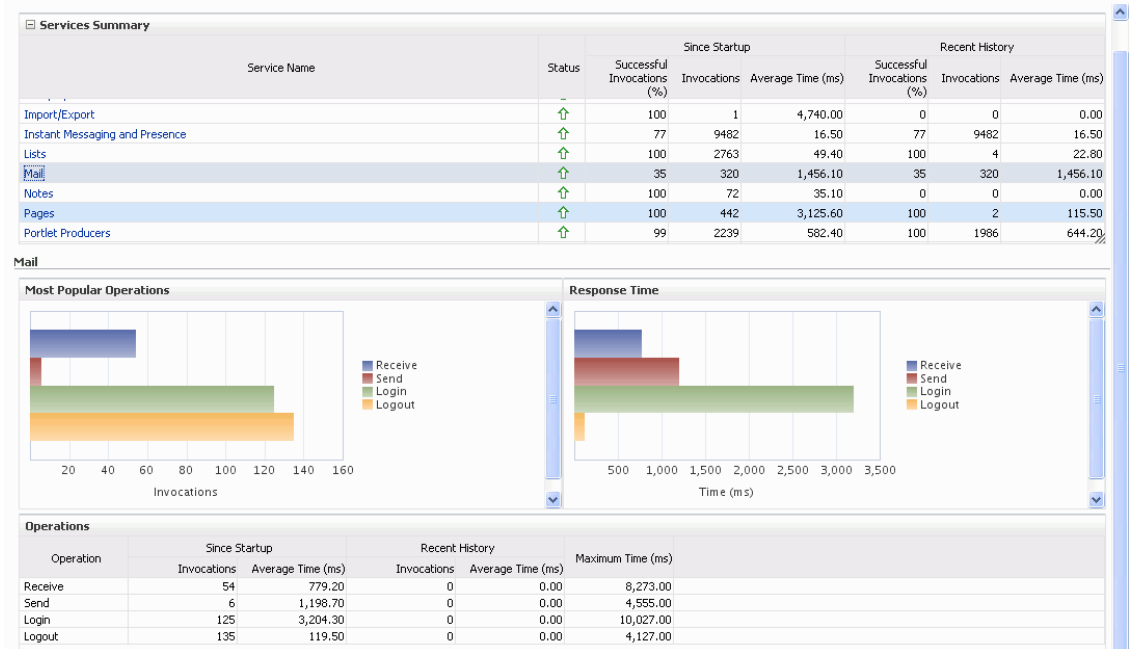
| <b>Operation</b> | <b>Description</b>   | <b>Performance Issues - User Action</b>  |
|------------------|--|--|
| Create Row       | Creates row of list data in the user session.  | For service-specific causes, see <a href="#">Section 15.1.5.9, "Lists Service."</a>  |
|                  | The Save Data operation commits list data changes to the WebCenter repository (the database where list data is stored).  | For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a>  |
| Update Row       | Updates row of list data in the user session.  | For service-specific causes, see <a href="#">Section 15.1.5.9, "Lists Service."</a>  |
|                  | The Save Data operation commits list data changes to the WebCenter repository (the database where list data is stored).  | For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a>  |
| Delete Row       | Deletes row of list data in the user session.  | For service-specific causes, see <a href="#">Section 15.1.5.9, "Lists Service."</a>  |
|                  | The Save Data operation commits list data changes to the WebCenter repository (the database where list data is stored).  | For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a>  |
| Search           | Retrieves a list by its ID from the Metadata Services (MDS) repository.  | For service-specific causes, see <a href="#">Section 15.1.5.9, "Lists Service."</a><br>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a> |
| Save Data        | Saves all changes to lists and list data (in the user session) to the Metadata Services (MDS) repository and the WebCenter repository (the database where list information is stored). | For service-specific causes, see <a href="#">Section 15.1.5.9, "Lists Service."</a><br>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a> |

#### 15.1.4.10 Mail Metrics

Performance metrics associated with the Mail service ([Figure 15–12](#)) are described in [Table 15–15](#) and [Section 15.1.2, "Overview of Common Metrics."](#)



**Figure 15–12 Mail Metrics**



To monitor these metrics through Fusion Middleware Control, see [Section 15.2, "Viewing Performance Information."](#)

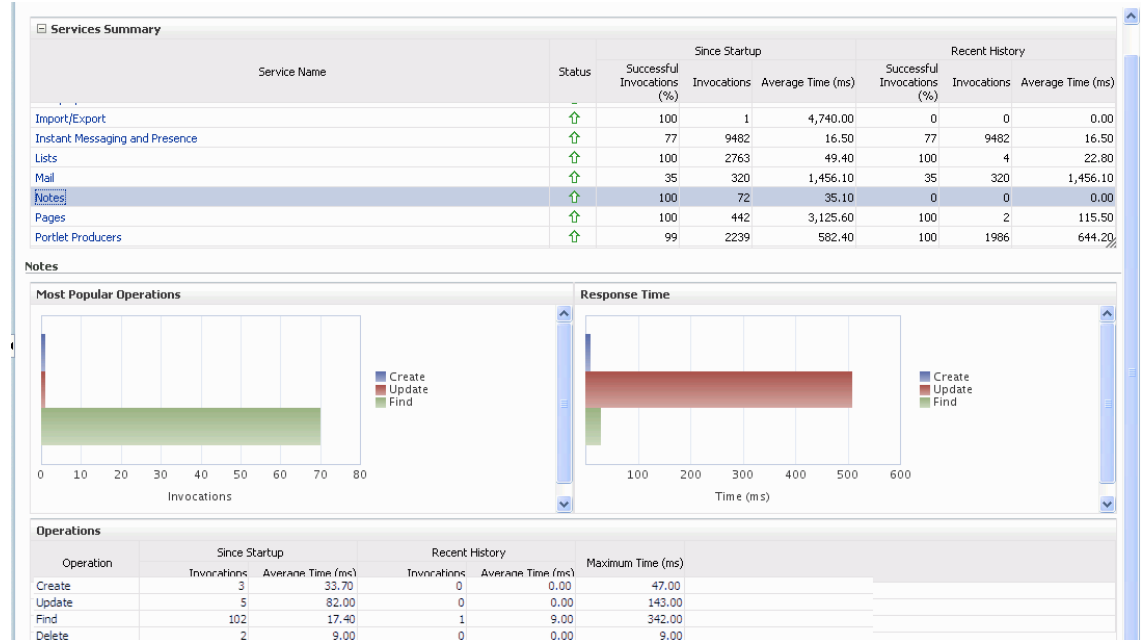
**Table 15–15 Mail Service - Operations Monitored**

| Operation | Description   | Performance Issues - User Action  |
|-----------|---|---|
| Login     | Logs a WebCenter user into the mail server that is hosting mail services.   | For service-specific causes, see <a href="#">Section 15.1.5.10, "Mail Service."</a><br>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a>                |
| Logout    | Logs a WebCenter user out of the mail server that is hosting mail services. | For service-specific causes, see <a href="#">Section 15.1.5.10, "Mail Service."</a><br>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a>                |
| Receive   | Receives a mail.  | For service-specific causes, see <a href="#">Section 15.1.5.10, "Mail Service."</a><br>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a>                |
| Send      | Sends a mail.   | For service-specific causes, see <a href="#">Section 15.1.5.10, "Mail Service."</a><br>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a>                |
| Search    | Searches for mail that contains a specific term.                            | For service-specific causes, see <a href="#">Section 15.1.5.10, "Mail Service."</a><br>For information on common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a> |

### 15.1.4.11 Note Metrics

Performance metrics associated with the Notes service (Figure 15–13) are described in Table 15–16 and Section 15.1.2, "Overview of Common Metrics."

**Figure 15–13 Notes Metrics**



To monitor these metrics through Fusion Middleware Control, see Section 15.2, "Viewing Performance Information."

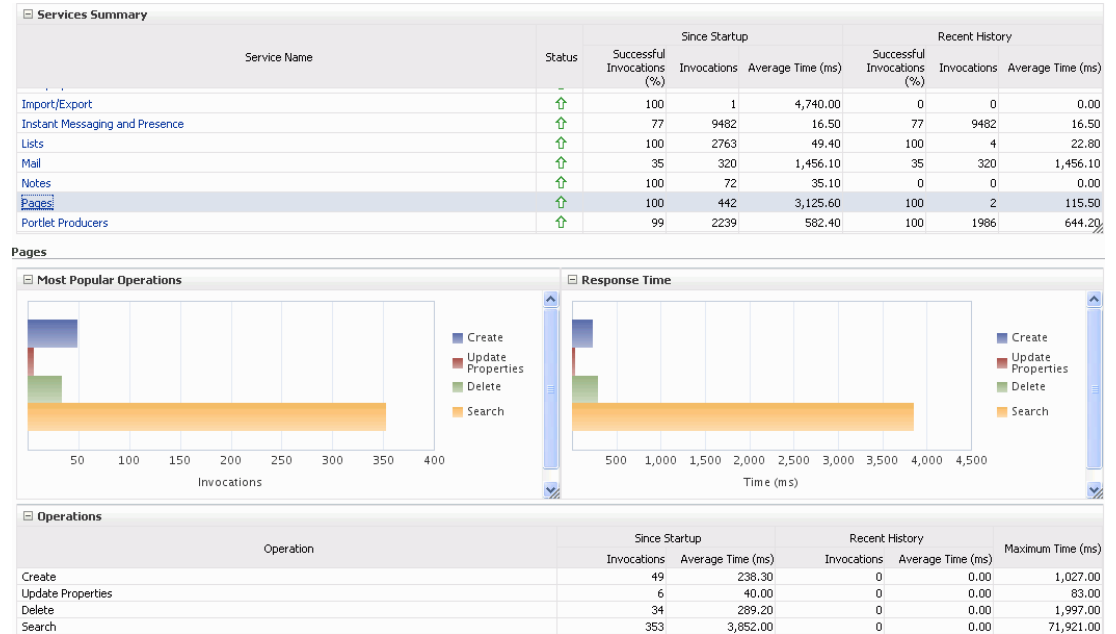
**Table 15–16 Notes Service - Operations Monitored**

| Operation | Description  | Performance Issues - User Action  |
|-----------|--|---|
| Create    | Creates a personal note.<br>The Save Changes operation commits new notes to the MDS repository.    | For service-specific causes, see Section 15.1.5.11, "Notes Service."<br>For common causes, see Section 15.1.3, "Common Performance Issues and Actions." |
| Update    | Updates a personal note.<br>The Save Changes operation commits note updates to the MDS repository. | For service-specific causes, see Section 15.1.5.11, "Notes Service."<br>For common causes, see Section 15.1.3, "Common Performance Issues and Actions." |
| Find      | Retrieves a note from the MDS repository.  | For service-specific causes, see Section 15.1.5.11, "Notes Service."<br>For common causes, see Section 15.1.3, "Common Performance Issues and Actions." |
| Delete    | Deletes a note from the MDS repository.  | For service-specific causes, see Section 15.1.5.11, "Notes Service."<br>For common causes, see Section 15.1.3, "Common Performance Issues and Actions." |

### 15.1.4.12 Page Metrics

Performance metrics associated with the Page service (Figure 15–14) are described in Table 15–17 and Section 15.1.2, "Overview of Common Metrics."

**Figure 15–14 Page Metrics**



To monitor these metrics through Fusion Middleware Control, see Section 15.2, "Viewing Performance Information."

**Table 15–17 Page Service - Operations Monitored**

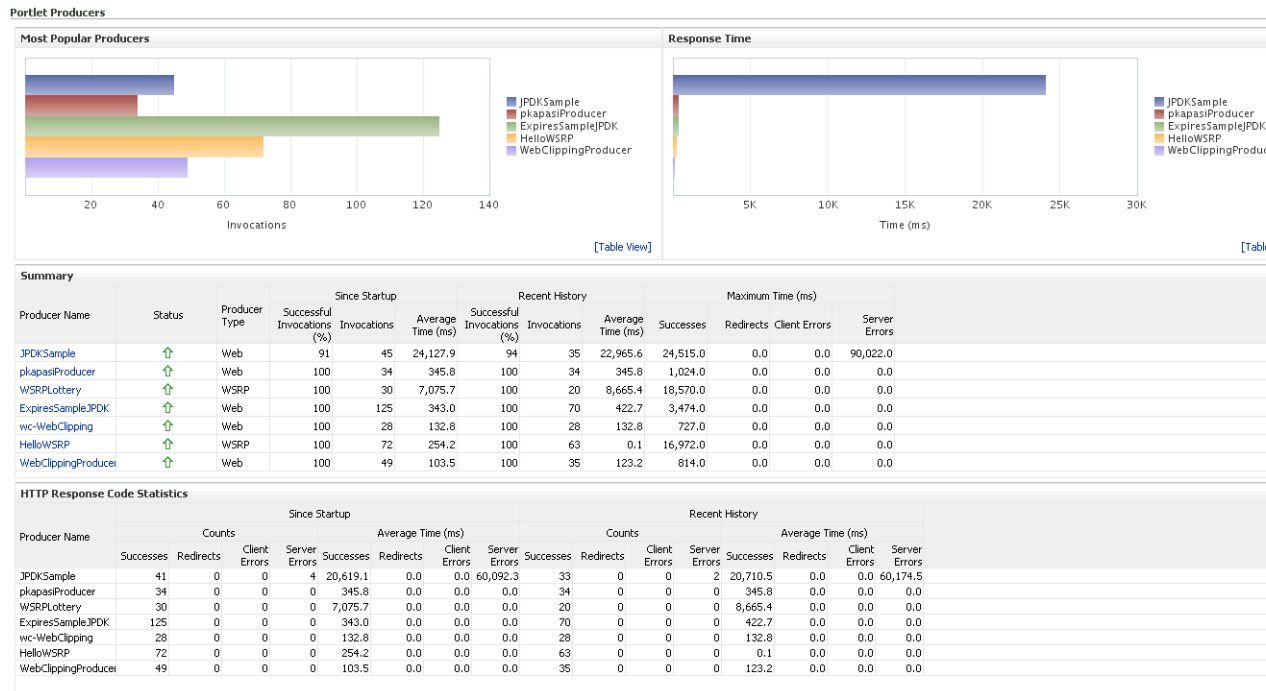
| Operation | Description                                      | Performance Issues - User Action   |
|-----------|--|--|
| Create    | Creates a page in the WebCenter application.     | For service-specific causes, see <a href="#">Section 15.1.5.12, "Page Service."</a><br>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a> |
| Copy      | Copies a page.                                   | For service-specific causes, see <a href="#">Section 15.1.5.12, "Page Service."</a><br>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a> |
| Delete    | Deletes a page.                                  | For service-specific causes, see <a href="#">Section 15.1.5.12, "Page Service."</a><br>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a> |
| Search    | Searches for pages that contain a specific term. | For service-specific causes, see <a href="#">Section 15.1.5.12, "Page Service."</a><br>For common causes, see <a href="#">Section 15.1.3, "Common Performance Issues and Actions."</a> |

### 15.1.4.13 Portlet Producer Metrics

Performance metrics associated with the portlet producers (Figure 15–15) are described in the following tables:

- [Table 15–18, "Portlet Producers - Summary"](#)
- [Table 15–19, "Portlet Producer -Detail"](#)

**Figure 15–15 Portlet Producer Metrics**



To monitor these metrics through Fusion Middleware Control, see [Section 15.2, "Viewing Performance Information."](#)

**Table 15–18 Portlet Producers - Summary**

| Metric | Description   |
|--------|---|
| Status | <p>The current status of portlet producers used in the WebCenter application:</p> <ul style="list-style-type: none"> <li>■ <b>Up</b> (Green Up Arrow) - Indicates that all portlet producers are up and running.</li> <li>■ <b>Down</b> (Red Down Arrow) - Indicates that the one or more portlet producers are currently unavailable. A producer instance might be down, or there could be some network connectivity issues.</li> <li>■ <b>Clock</b> - Unable to query the status of the portlet producers for some reason.</li> </ul> |

**Table 15–18 (Cont.) Portlet Producers - Summary**

| <b>Metric</b>              | <b>Description</b>  |
|----------------------------|---|
| Successful Invocations (%) | <p>The percentage of portlet producer invocations that succeeded:</p> <ul style="list-style-type: none"> <li>- Since Startup</li> <li>- Recent History</li> </ul> <p>Any request that fails will impact availability. This includes WebCenter application-related failures such as timeouts and internal errors, as well as remote/server failures such as requests returned with response codes HTTP4xx or HTTP5xx, responses with a bad content type, and SOAP faults, where applicable.</p> <p>If Successful Invocations (%) is below 100%, check the diagnostic logs to establish why service requests are failing. See, <a href="#">Section 15.3, "Viewing and Configuring Log Information."</a></p> |
| Invocations                | <p>The number of portlet producer invocations per minute:</p> <ul style="list-style-type: none"> <li>- Since Startup</li> <li>- Recent History</li> </ul> <p>This metric measures each WebCenter application-related portlet request and therefore, due to cache hits, errors, or timeouts on the application, this total may be higher than the number of actual HTTP requests made to the producer server.</p>  |
| Average Time (ms)          | <p>The average time taken to make a portlet request, regardless of the result:</p> <ul style="list-style-type: none"> <li>- Since Startup</li> <li>- Recent History</li> </ul>  |

**Table 15–19 Portlet Producer -Detail**

| <b>Metric</b>          | <b>Description</b>  |
|------------------------|---|
| Most Popular Producers | <p>The number of invocations per producer (displayed on a chart).</p> <p>The highest value on the chart indicates which portlet producer is used the most.</p> <p>The lowest value indicates which portlet producer is used the least.</p>  |
| Response Time          | <p>The average time each portlet producer takes to process producer requests since the WebCenter application started up (displayed on a chart).</p> <p>The highest value on the chart indicates the worst performing portlet producer.</p> <p>The lowest value indicates which portlet producer is performing the best.</p> |
| Producer Name          | <p>The name of the portlet producer being monitored.</p> <p>Click the name of a portlet producer to pop up more detailed information about each portlet that the application uses. See also <a href="#">Table 15–21, "Portlet - Detail"</a>.</p>  |

**Table 15–19 (Cont.) Portlet Producer -Detail**

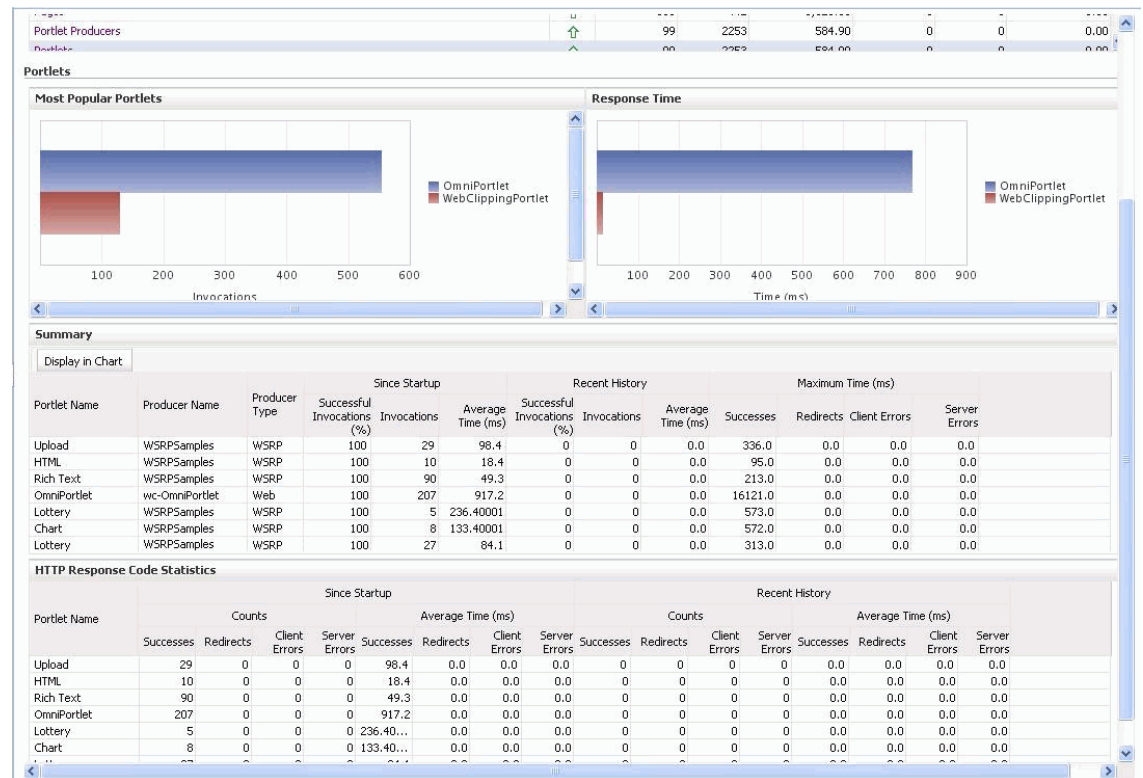
| <b>Metric</b>              | <b>Description</b>   |
|----------------------------|--|
| Status                     | <p>The current status of each portlet producer:</p> <ul style="list-style-type: none"> <li>■ <b>Up</b> (Green Up Arrow) - Indicates that the portlet producer is up and running.</li> <li>■ <b>Down</b> (Red Down Arrow) - Indicates that the portlet producer is currently unavailable. The producer instance might be down, or there could be some network connectivity issues.</li> <li>■ <b>Clock</b> - Unable to query the status of portlet producer for some reason.</li> </ul> |
| Producer Type              | <p>The portlet producer type: Web or WSRP</p> <ul style="list-style-type: none"> <li>■ Web portlet producer - deployed to a J2EE application server, which is often remote and communicates through Simple Object Access Protocol (SOAP) over HTTP.</li> <li>■ WSRP portlet producer - Web Services for Remote Portlets (WSRP) is a Web services standard that allows interoperability between a standards enabled container and any WSRP application.</li> </ul>                      |
| Successful Invocations (%) | <p>The percentage of producer invocations that succeeded:</p> <ul style="list-style-type: none"> <li>- Since Startup</li> <li>- Recent History</li> </ul>  |
| Invocations                | <p>The number of invocations, per producer:</p> <ul style="list-style-type: none"> <li>- Since Startup</li> <li>- Recent History</li> </ul> <p>By sorting the table on this column, you can find the most frequently accessed portlet producer in your WebCenter application.</p>  |
| Average Time (ms)          | <p>The average time taken to make a portlet request, regardless of the result:</p> <ul style="list-style-type: none"> <li>- Since Startup</li> <li>- Recent History</li> </ul> <p>Use this metric to detect non-functional portlet producers. If you use this metric in conjunction with the Invocations metric, then you can prioritize which producer to focus on.</p>   |
| Maximum Time (ms)          | <p>The maximum time taken to process producer requests:</p> <ul style="list-style-type: none"> <li>- Successes - HTTP200xx response code</li> <li>- Re-directs - HTTP300xx response code</li> <li>- Client Errors - HTTP400xx response code</li> <li>- Server Errors - HTTP500xx response code</li> </ul>  |

#### 15.1.4.14 Portlet Metrics

Performance metrics associated with portlets (Figure 15–16) are described in the following tables:

- [Table 15–20, "Portlets - Summary"](#)
- [Table 15–21, "Portlet - Detail"](#)
- [Table 15–22, "Portlet - HTTP Response Code Statistics"](#)
- [Table 15–23, "HTTP Response Codes"](#)

Figure 15–16 Portlet Metrics



To monitor these metrics through Fusion Middleware Control, see [Section 15.2, "Viewing Performance Information."](#)

Table 15–20 Portlets - Summary

| Metric                     | Description  |
|----------------------------|--|
| Status                     | <p>The current status of portlets used in the WebCenter application:</p> <ul style="list-style-type: none"> <li>■ <b>Up</b> (Green Up Arrow) - Indicates that all portlets are up and running.</li> <li>■ <b>Down</b> (Red Down Arrow) - Indicates that the one or more portlets are currently unavailable. A producer instance might be down, or there could be some network connectivity issues. For other causes, see <a href="#">Section 15.1.5.13, "Portlets and Producers."</a></li> <li>■ <b>Clock</b> - Unable to query the status of portlets for some reason.</li> </ul> |
| Successful Invocations (%) | <p>The percentage of portlet invocations that succeeded:</p> <ul style="list-style-type: none"> <li>- Since Startup</li> <li>- Recent History</li> </ul> <p>Any request that fails will impact availability. This includes WebCenter application-related failures such as timeouts and internal errors, as well as client/server errors.</p> <p>If Successful Invocations (%) is below 100%, check the diagnostic logs to establish why service requests are failing. See, <a href="#">Section 15.3, "Viewing and Configuring Log Information."</a></p>                            |

**Table 15–20 (Cont.) Portlets - Summary**

| <b>Metric</b>     | <b>Description</b>   |
|-------------------|--|
| Invocations       | <p>The number of portlet invocations per minute:</p> <ul style="list-style-type: none"> <li>- Since Startup</li> <li>- Recent History</li> </ul> <p>This metric measures each WebCenter application-related portlet request and therefore, due to cache hits, errors, or timeouts on the application, this total may be higher than the number of actual HTTP requests made to the portlet producer.</p> |
| Average Time (ms) | <p>The average time taken to process operations associated with portlets, regardless of the result:</p> <ul style="list-style-type: none"> <li>- Since Startup</li> <li>- Recent History</li> </ul>  |

**Table 15–21 Portlet - Detail**

| <b>Metric</b>              | <b>Description</b>  |
|----------------------------|---|
| Most Popular Portlets      | <p>The number of invocations per portlet (displayed on a chart).<br/>The highest value on the chart indicates which portlet is used the most.<br/>The lowest value indicates which portlet is used the least.</p>   |
| Response Time              | <p>The average time each portlet takes to process requests since the WebCenter application started up (displayed on a chart).<br/>The highest value on the chart indicates the worst performing portlet.<br/>The lowest value indicates which portlet is performing the best.</p>   |
| Portlet Name               | The name of the portlet being monitored.  |
| Status                     | <p>The current status of each portlet:</p> <ul style="list-style-type: none"> <li>■ <b>Up</b> (Green Up Arrow) - Indicates that the portlet is up and running.</li> <li>■ <b>Down</b> (Red Down Arrow) - Indicates that the portlet is currently unavailable. The producer instance might be down, or there could be some network connectivity issues.</li> </ul>   |
| Producer Name              | The name of the portlet producer through which the portlet is accessed.   |
| Producer Type              | <p>The portlet producer type: Web or WSRP</p> <ul style="list-style-type: none"> <li>■ Web portlet producer - deployed to a J2EE application server, which is often remote and communicates through Simple Object Access Protocol (SOAP) over HTTP.</li> <li>■ WSRP portlet producer - Web Services for Remote Portlets (WSRP) is a Web services standard that allows interoperability between a standards enabled container and any WSRP application.</li> </ul> |
| Successful Invocations (%) | <p>The percentage of portlet invocations that succeeded:</p> <ul style="list-style-type: none"> <li>- Since Startup</li> <li>- Recent History</li> </ul> <p>If Successful Invocations (%) is below 100%, check the diagnostic logs to establish why service requests are failing. See, <a href="#">Section 15.3, "Viewing and Configuring Log Information."</a></p>   |



**Table 15–21 (Cont.) Portlet - Detail**

| <b>Metric</b>     | <b>Description</b>  |
|-------------------|---|
| Invocations       | <p>The number of invocations, per portlet:</p> <ul style="list-style-type: none"> <li>- Since Startup</li> <li>- Recent History</li> </ul> <p>By sorting the table on this column, you can find the most frequently accessed portlet in your WebCenter application.</p>   |
| Average Time (ms) | <p>The average time each portlet takes to process requests, regardless of the result:</p> <ul style="list-style-type: none"> <li>- Since Startup</li> <li>- Recent History</li> </ul> <p>Use this metric to detect non-performant portlets. If you use this metric in conjunction with the Invocations metric, then you can prioritize which portlet to focus on.</p>   |
| Maximum Time (ms) | <p>The maximum time taken to process portlet requests:</p> <ul style="list-style-type: none"> <li>- Successes - HTTP200xx</li> <li>- Redirects - HTTP300xx</li> <li>- Client Errors - HTTP400xx</li> <li>- Server Errors - HTTP500xx</li> </ul> <p>The breakdown of performance statistics by HTTP response code can help you identify which factors are driving up the total average response time. For example, failures due to portlet producer timeouts would adversely affect the total average response time.</p> |

**Table 15–22 Portlet - HTTP Response Code Statistics**

| <b>Metric</b>     | <b>Description</b>   |
|-------------------|--|
| Portlet Name      | The name of the portlet being monitored.   |
| Invocations Count | The number of invocations, by type (HTTP response code):   |
| - Successes       | - Since Startup  |
| - Redirects       | - Recent History   |
| - Client Errors   | See also, <a href="#">Table 15–23, "HTTP Response Codes"</a> .   |
| - Server Errors   |  |
| Average Time (ms) | The average time each portlet takes to process requests:   |
| - Successes       | - Since Startup  |
| - Redirects       | - Recent History   |
| - Client Errors   | Use this metric to detect non-functional portlets. If you use this metric in conjunction with the Invocations metric, then you can prioritize which portlet to focus on. |
| - Server Errors   |  |

**Table 15–23 HTTP Response Codes**

| <b>HTTP Response and Error Code</b> | <b>Description</b>   |
|-------------------------------------|--|
| 200 -Successful Requests            | Portlet requests that return any HTTP2xx response code, or which were successful without requiring an HTTP request to the remote producer, for example, a cache hit. |

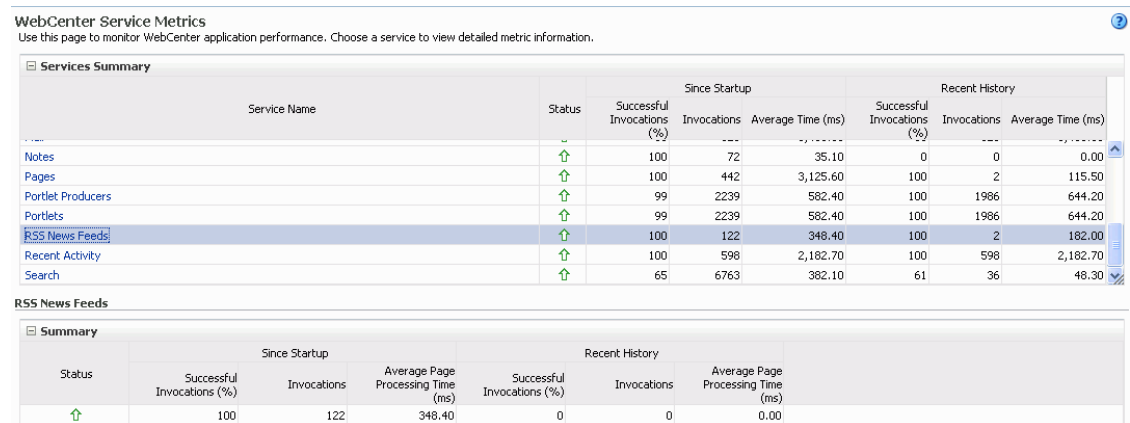
**Table 15–23 (Cont.) HTTP Response Codes**

| HTTP Response and Error Code         | Description  |
|--------------------------------------|--|
| 300 -Unresolved Redirections         | Portlet requests that return any HTTP3xx response code.  |
| 400 -Unsuccessful Request Incomplete | Portlet requests that return any HTTP4xx response code.  |
| 500 -Unsuccessful Server Errors      | Portlet requests that failed for any reason, including requests that return HTTP5xx response codes, or which failed due to a WebCenter application-related error, timeout, bad content type response, or SOAP fault. |

**15.1.4.15 RSS News Feed Metrics**

Performance metrics associated with the RSS service (Figure 15–17) are described in Section 15.1.2, "Overview of Common Metrics."

**Figure 15–17 RSS News Feed Metrics**

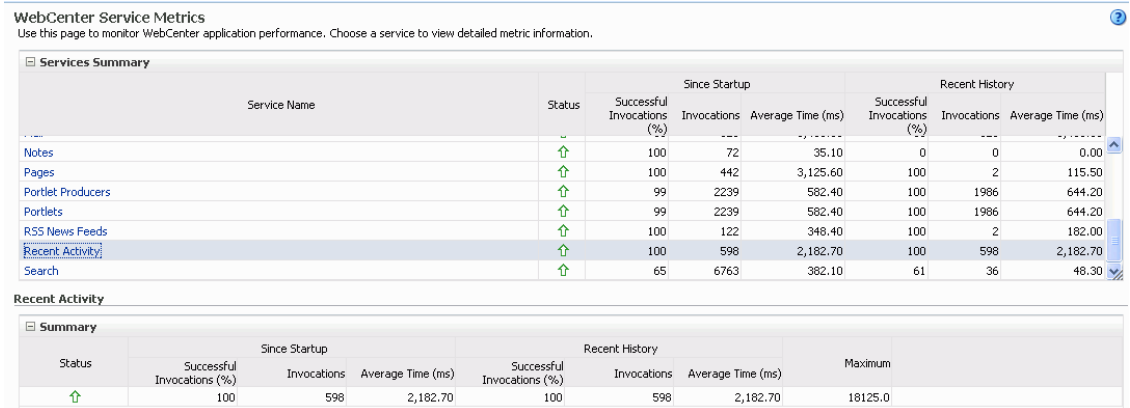


To monitor these metrics through Fusion Middleware Control, see Section 15.2, "Viewing Performance Information."

**15.1.4.16 Recent Activity Metrics**

Performance metrics associated with the Recent Activities service (Figure 15–18) are described in Section 15.1.2, "Overview of Common Metrics."

**Figure 15–18 Recent Activity Metrics**

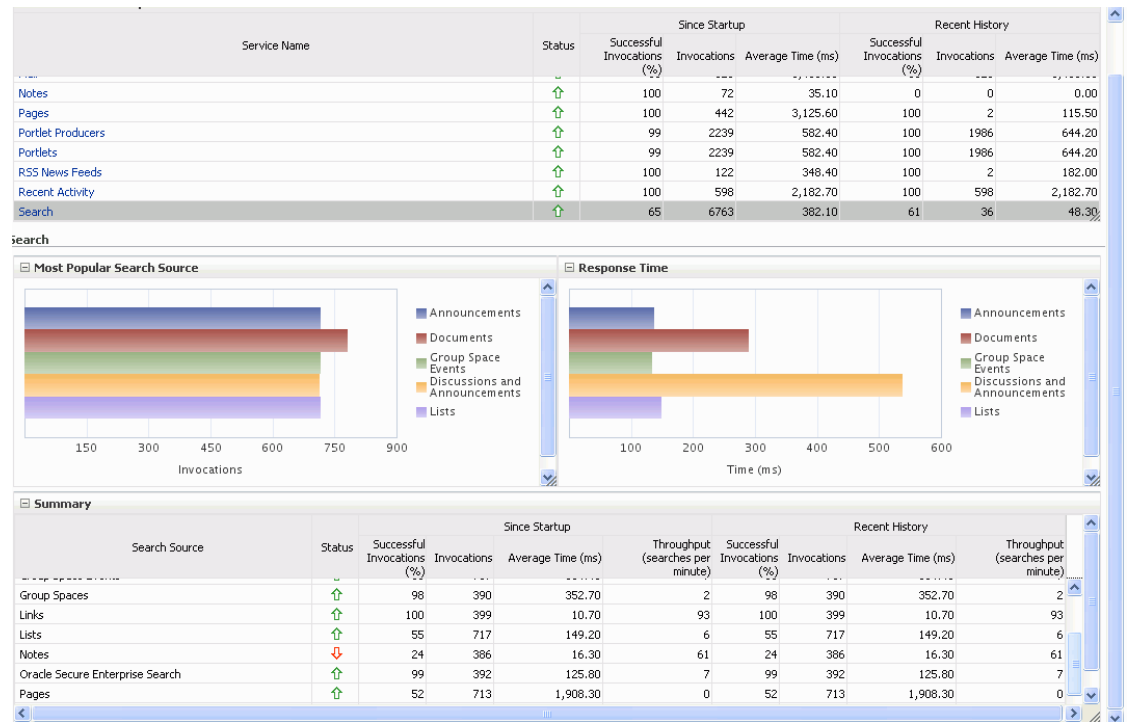


To monitor these metrics through Fusion Middleware Control, see [Section 15.2, "Viewing Performance Information."](#)

**15.1.4.17 Search Metrics**

Performance metrics associated with the Search service ([Figure 15–19](#)) are described in [Table 15–24](#) and [Section 15.1.2, "Overview of Common Metrics."](#)

**Figure 15–19 Search Metrics**



To monitor these metrics through Fusion Middleware Control, see [Section 15.2, "Viewing Performance Information."](#)

**Table 15–24 Search Service - Search Sources**

| Operation     | Description                    |
|---------------|--------------------------------|
| Announcements | Announcement text is searched. |

**Table 15–24 (Cont.) Search Service - Search Sources**

| Operation                       | Description  |
|---------------------------------|--|
| Documents                       | Contents in files and folders are searched.  |
| Discussion Forums               | Forums and topics are searched.  |
| Group Spaces                    | Contents saved in a group space, such as links, lists, notes, tags, and group space events are searched.                           |
| Group Space Events              | Group space events are searched.   |
| Links                           | Objects to which links have been created are searched. For example, announcements, discussion forum topics, documents, and events. |
| Lists                           | Information stored in lists is searched.   |
| Notes                           | Notes text, such as reminders, is searched.  |
| Oracle Secure Enterprise Search | Contents from the Document Library task flow, discussions, tag clouds, notes, and other WebCenter services are searched.           |
| Pages                           | Contents added to application, personal, public, wiki, and blog pages are searched.  |

### 15.1.5 Service-Specific Performance Issues and Actions

This section describes service-specific performance issues and user actions required to address those issue. This section includes the following sub sections:

---



---

**Note:** For information about troubleshooting Web 2.0 Services, see [Appendix B, "Troubleshooting"](#). For information about tuning the performance of Web 2.0 Services, see [Appendix A, "WebCenter Configuration."](#)

---



---

- [Announcements Service](#)
- [BPEL Worklist Service](#)
- [Content Repository \(Documents\) Service](#)
- [Discussions Service](#)
- [External Applications Service](#)
- [Group Space Events Service](#)
- [Instant Messaging and Presence \(IMP\) Service](#)
- [Import and Export](#)
- [Lists Service](#)
- [Mail Service](#)
- [Notes Service](#)
- [Page Service](#)
- [Portlets and Producers](#)
- [RSS News Feed Service](#)
- [Recent Activities Service](#)
- [Search Service](#)

### 15.1.5.1 Announcements Service

If you are facing problems with the Announcements service and the status is **Down**, check the diagnostic logs to establish why this service is unavailable. Some typical causes of failure include:

- Back-end Discussions server is down or not responding.
- Network connectivity issues exist between the application and the back-end discussion server.
- Connection configuration information associated with the Announcements service is incorrect or no longer valid.

### 15.1.5.2 BPEL Worklist Service

If you are facing problems with the BPEL Worklist service and the status is **Down**, check the diagnostic logs to establish why this service is unavailable. Some typical causes of failure include:

- BPEL server being queried is not available.
- Network connectivity issues exist between the application and the BPEL Server.
- Connection configuration information associated with the Worklist service is incorrect or no longer valid.

### 15.1.5.3 Content Repository (Documents) Service

If you are facing problems with the Documents service and the status is **Down**, check the diagnostic logs to establish why this service is unavailable. Also, do one of the following:

- For Oracle Content Server and Oracle Portal, verify that the back-end server is up and running.
- For Oracle Content Server, verify that the socket connection is open for the client for which the service is not functioning properly.
- For Oracle Portal, verify the status of the JDBC connection using Oracle WebLogic Administration Console.
- (Functional check) Check logs on the back-end server. For Oracle Content Server, go to Oracle Content Server > Administration > Log files > Content Server Logs. For Oracle Portal use Fusion Middleware Control.
- (Functional check) Search for log entries in which the module name starts with `oracle.vcr`, `oracle.webcenter.content`, `oracle.webcenter.doclib`, and `oracle.stellent`.

### 15.1.5.4 Discussions Service

If you are facing problems with the Discussions service and the status is **Down**, check the diagnostic logs to establish why this service is unavailable. Some typical causes of failure include:

- Back-end discussions server is down or not responding.
- Network connectivity issues exist between the application and the back-end discussion server.
- Connection configuration information associated with the Discussions service is incorrect or no longer valid.

#### 15.1.5.5 External Applications Service

If you are facing problems with the External Applications service and the status is **Down**, check the diagnostic logs to establish why this service is unavailable. Some typical causes of failure include:

- Credential store is not configured for the application.
- Credential store that is configured, for example LDAP, is down or not responding.

#### 15.1.5.6 Group Space Events Service

If you are facing problems with the Group Space Events service and the status is **Down**, check the diagnostic logs to establish why this service is unavailable. Some typical causes of failure include:

- WebCenter repository is not available (the database where event information is stored).
- Network connectivity issues exist between the application and the WebCenter repository.
- Connection configuration information associated with the Group Space Events service is incorrect or no longer valid.

#### 15.1.5.7 Instant Messaging and Presence (IMP) Service

If you are facing problems with the IMP service and the status is **Down**, check the diagnostic logs to establish why this service is unavailable. Some typical causes of failure include:

- Instant Messaging and Presence server is not available.
- Network connectivity issues exist between the application and the Instant Messaging and Presence server.
- Connection configuration information associated with the IMP service is incorrect or no longer valid.

#### 15.1.5.8 Import and Export

If you are facing import and export problems and the status is **Down**, check the diagnostic logs to establish why this service is unavailable.

#### 15.1.5.9 Lists Service

If you are facing problems with the Lists service and the status is **Down**, check the diagnostic logs to establish why this service is unavailable. Some typical causes of failure include:

- MDS repository or WebCenter repository in which the data of the Lists service is stored, is not available.
- Network connectivity issues exist between the application and the repository.
- Connection configuration information associated with the Lists service is incorrect or no longer valid.

#### 15.1.5.10 Mail Service

If you are facing problems with the Mail service and the status is **Down**, check the diagnostic logs to establish why this service is unavailable. Some typical causes of failure include:

- Mail server is not available.
- Network connectivity issues exist between the application and the mail server.
- Connection configuration information associated with the Mail service is incorrect or no longer valid.

#### 15.1.5.11 Notes Service

If you are facing problems with the Notes service, verify if the MDS repository is not available or responding slowly (the repository where note information is stored).

#### 15.1.5.12 Page Service

If you are facing problems with the Page service and the status is **Down**, check the diagnostic logs to establish why this service is unavailable. Some typical causes of failure include:

- WebCenter repository is not available (the database where page information is stored).
- Network connectivity issues exist between the application and the WebCenter repository.

#### 15.1.5.13 Portlets and Producers

If you are facing problems with a portlet producer and the status is **Down**, check the diagnostic logs to establish why this service is unavailable. Some typical causes of failure include:

- Portlet producer server is down or not responding.
- Connection configuration information associated with the portlet producer is incorrect or no longer valid.
- Producer requests are timing out.
- There may be a problem with a particular producer, or the performance issue is due to a specific portlet(s) from that producer.

#### 15.1.5.14 RSS News Feed Service

If you are facing problems with the RSS News Feed service and the status is **Down**, check the diagnostic logs to establish why this service is unavailable. Some typical causes of failure include:

- The Search service is not available.
- A service being searched for recent activities has failed

#### Unable to Get Discussions Data

If you are experiencing performance issues, check the performance of the Discussions service.

#### Unable to Get Lists Data

If you are experiencing performance issues, check the performance of the Lists service.

#### Unable to Get Recent Activities Data

If you are experiencing performance issues, check the performance of the Recent Activity service.

### 15.1.5.15 Recent Activities Service

If you are facing problems with the Recent Activities service and the status is **Down**, check the diagnostic logs to establish why this service is unavailable. Some typical causes of failure include:

- Search Service is not available.
- A service being searched for recent activity has failed

### 15.1.5.16 Search Service

If you are facing problems with the Search service (a service executor) and the status is **Down**, check the diagnostic logs to establish why this executor is unavailable. Some typical causes of failure include:

- The repository of the executor is not available.
- Network connectivity issues exist between the application and the repository of the executor.
- Connection configuration information associated with the executor is incorrect or no longer valid.
- Content repositories being searched is currently unavailable.

## 15.1.6 Group Space Metrics

(WebCenter Spaces only) Performance metrics associated with group space activity (Figure 15–20) are described in Table 15–25 and Section 15.1.2, "Overview of Common Metrics."

Figure 15–20 Group Space Metrics





To monitor these metrics through Fusion Middleware Control, see [Section 15.2, "Viewing Performance Information."](#)

**Table 15–25 Group Space Metrics**

| <b>Metric</b>                  | <b>Description</b>  |
|--------------------------------|---|
| WebCenter Spaces URL           | The WebCenter Spaces application being managed.   |
| WebLogic Server                | The WebLogic Server instance in which WebCenter Spaces is deployed.   |
| J2EE Application               | The name of the WebCenter Spaces application.   |
| Group Space Page Response      | The current average response time (in milliseconds) of group space pages.   |
| Most Popular Group Spaces      | Graph showing the most popular group spaces, that is, group spaces recording the most invocations.<br>To compare a different set of group spaces, select one or more group spaces in the table, and then click <b>Display in Chart</b> .  |
| Group Space Page Throughput    | Graph showing the average number of pages processed per minute for each group space.<br>To compare a different set of group spaces, select one or more group spaces in the table, and then click <b>Display in Chart</b> .  |
| Group Space Page Response Time | Graph showing the average page response time (in milliseconds) per group space.<br>To compare a different set of group spaces, select one or more group spaces in the table, and then click <b>Display in Chart</b> .   |
| Status                         | The current status of each group space: <ul style="list-style-type: none"> <li>■ <b>Up</b> (Green Up Arrow) - Indicates that the last group space operation was successful. The group space is up and running.</li> <li>■ <b>Down</b> (Red Down Arrow) - Indicates that the group space is not currently available or the last group space operation was unsuccessful due to an unexpected error or exception. User errors, such as an authentication failure, do not change the status to "Down".</li> </ul> |
| Successful Invocations (%)     | The percentage of group space invocations that succeeded: <ul style="list-style-type: none"> <li>- Since Startup</li> <li>- Recent History</li> </ul> <p>If Successful Invocations (%) is below 100%, check the diagnostic logs to establish why service requests are failing. See, <a href="#">Section 15.3, "Viewing and Configuring Log Information."</a></p>  |
| Invocations                    | The number of group space invocations per minute: <ul style="list-style-type: none"> <li>- Since Startup</li> <li>- Recent History</li> </ul>   |
| Page Throughput                | The average number of pages processed per minute for each group space: <ul style="list-style-type: none"> <li>- Since Startup</li> <li>- Recent History</li> </ul>  |
| Average Time (ms)              | The average time (in ms) to display group space pages: <ul style="list-style-type: none"> <li>- Since Startup</li> <li>- Recent History</li> </ul>  |
| Maximum Time (ms)              | The maximum time taken to display a group space page.   |

**Table 15–25 (Cont.) Group Space Metrics**

| Metric            | Description   |
|-------------------|---|
| Minimum Time (ms) | The minimum time taken to display a group space page. |

## 15.2 Viewing Performance Information

Fusion Middleware Control monitors a wide range of performance metrics for WebCenter applications. You can view performance data for all the dependent services, external applications, and portlet producers used by your WebCenter application.

This section includes the following sub sections:

- [Monitoring WebCenter Spaces](#)
- [Monitoring Custom WebCenter Applications](#)

### 15.2.1 Monitoring WebCenter Spaces

Administrators can monitor the performance and availability of all the components and services that make up WebCenter Spaces, as well as the application as a whole. These detailed metrics will help diagnose performance issues and, if monitored regularly, you will learn to recognize trends as they develop and prevent performance problems in the future.

Some key metrics display on the WebCenter Spaces home page. You can see at a glance which group spaces are the most popular, identify the best and worst performing group spaces and more. For details, see [Section 15.1.6, "Group Space Metrics"](#).

The WebCenter Spaces Home page also summarizes the status and performance of individual services, external applications, and any portlet producers that the application uses. When a service is **Down** or running slowly you can drill down to more detailed metrics to troubleshoot the problem, and take corrective action. For metric information, see [Section 15.1, "Understanding WebCenter Performance Metrics."](#)

To access performance metrics for WebCenter Spaces:

1. In Fusion Middleware Control Console, navigate to the home page for WebCenter Spaces.

See [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#).

2. From the **WebCenter** menu, choose **Monitoring > Service Metrics**.

Use **Services Summary** at the top of the **WebCenter Service Metrics** page to quickly see which services are up and running, and to review individual and relative performances of those services used by WebCenter Spaces.

Statistics become available when a service, application, or portlet is accessed for the first time. If a service is not configured or has never been used it will not appear in the **Summary** table.

3. Click the name of a service to drill down to more detailed metrics.

To learn more about individual metrics, see [Section 15.1, "Understanding WebCenter Performance Metrics"](#).

To access performance summary for WebCenter Spaces:

1. In Fusion Middleware Control Console, navigate to the home page for WebCenter Spaces.

See [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#).

2. From the **WebCenter** menu, choose **Monitoring > Performance Summary**.

Use the **Show Metric Palette** button at the top of the **Performance Summary** page to display the **Metric Palette**. This palette enables you to select metrics for services that are up and running, and to review live performances of individual services in graphical and tabular formats.

Statistics become available when a service, application, or portlet is accessed for the first time. If a service is not configured or has never been used it will not appear in the performance summary graphs and tables.

3. In the **Metric Palette**, expand a service folder and select the metric checkboxes to view the service performance in graphical or tabular format.

## 15.2.2 Monitoring Custom WebCenter Applications

Administrators can monitor the performance and availability of all the components and services that make up custom WebCenter applications, as well as the application as a whole. These detailed metrics will help diagnose performance issues and, if monitored regularly, you will learn to recognize trends as they develop and prevent performance problems in the future.

To access performance metrics for a custom WebCenter application:

1. In Fusion Middleware Control Console, navigate to the home page for custom WebCenter applications.

See [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#).

2. From the **Application Deployment** menu, choose **WebCenter > Service Metrics**.

Use the **Services Summary** at the top of the **WebCenter Service Metrics** page to quickly see which services are up and running, and to review individual and relative performances of all the services used by the WebCenter application.

Statistics become available when a service, application, or portlet is accessed for the first time. If a service is not configured or has never been used it will not appear in the Services Summary table.

3. Click the name of a service to drill down to more detailed metrics.

To learn more about individual metrics for each service, see [Section 15.1, "Understanding WebCenter Performance Metrics"](#).

To access performance summary for a custom WebCenter application:

1. In Fusion Middleware Control Console, navigate to the home page for custom WebCenter applications.

See [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#).

2. From the **Application Deployment** menu, choose **Performance Summary**.

Use the **Show Metric Palette** button at the top of the **Performance Summary** page to display the **Metric Palette**. This palette enables you to select metrics for services that are up and running, and to review live performances of individual services in graphical and tabular formats.

Statistics become available when a service, application, or portlet is accessed for the first time. If a service is not configured or has never been used it will not appear in the performance summary graphs and tables.

3. In the **Metric Palette**, expand a service folder and select the metric checkboxes to view the service performance in graphical or tabular format.

## 15.3 Viewing and Configuring Log Information

All diagnostic information related to startup and shutdown information, errors, warning messages, access information on HTTP requests, and additional information get stored in log files. To learn how to find information about the cause of an error and its corrective action, see the chapter "Managing Log Files and Diagnostic Data" in *Oracle Fusion Middleware Administrator's Guide*. To learn how to enable diagnostic logging to identify issues, see the section "Configuring Settings for Log Files" in *Oracle Fusion Middleware Administrator's Guide*.

For WebCenter Spaces, the log file, `WLS_Spaces-diagnostic.log` is stored in the `DOMAIN_HOME/servers/WLS_Spaces/logs` directory.

For custom WebCenter applications, the log file is available in the `DOMAIN_HOME/servers/ServerName/logs` directory. The log file follows the naming convention of `ServerName-diagnostics.log`.

For example, for a managed server, `WLS_Custom`, the logs will be stored in the `DOMAIN_HOME/servers/WLS_Custom/logs`, and the log file name will be `WLS_Custom-diagnostics.log`.

This section includes the following sub sections:

- [WebCenter Spaces Logs](#)
- [Custom WebCenter Application Logs](#)

### 15.3.1 WebCenter Spaces Logs

To view log messages in WebCenter Spaces:

1. In Fusion Middleware Control Console, navigate to the home page for WebCenter Spaces.  
See [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#).
2. From the **WebCenter** menu, choose **Logs > View Log Messages**.
3. In the **Log Messages** page, search for warnings, errors, notifications, and so on.

To configure log files in WebCenter Spaces:

1. In Fusion Middleware Control Console, navigate to the home page for WebCenter Spaces.  
See [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#).
2. From the **WebCenter** menu, choose **Logs > Log Configuration**.
3. In the **Log Configuration** page, in the **Log Files** tab, configure log settings.

For more information, see the section "Searching and Viewing Log Files" in *Oracle Fusion Middleware Administrator's Guide*.

## 15.3.2 Custom WebCenter Application Logs

To view log messages in custom WebCenter applications:

1. In Fusion Middleware Control Console, navigate to the home page for WebCenter applications.

See [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#).

2. From the **Application Deployment** menu, choose **Logs > View Log Messages**.
3. In the **Log Messages** page, search for warnings, errors, notifications, and so on.

To configure log files in custom WebCenter applications:

1. In Fusion Middleware Control Console, navigate to the home page for WebCenter applications.

See [Section 6.3, "Navigating to the Home Page for Custom WebCenter Applications"](#).

2. From the **Application Deployment** menu, choose **Logs > Log Configuration**.
3. In the **Log Configuration** page, in the **Log Files** tab, configure log settings.

For more information, see the section "Searching and Viewing Log Files" in *Oracle Fusion Middleware Administrator's Guide*.



---

## Managing Export, Import, Backup, and Recovery of WebCenter

Oracle WebCenter stores data related to its configuration and content for the various feature areas in a number of locations. To facilitate disaster recovery and the full production lifecycle from development through staging and production, WebCenter provides a set of utilities that enable you to back up this data, move the data between WebCenter applications in staging and production environments. This chapter describes the backup, import, and export capabilities and tools available. It includes the following sections:

- [Exporting and Importing WebCenter Spaces for Data Migration](#)
- [Exporting and Importing Custom WebCenter Applications for Data Migration](#)
- [Backing Up and Recovering WebCenter Applications](#)

To best plan the proper usage of these tools, note down which WebCenter features your WebCenter applications are using: WebCenter Framework, WebCenter Spaces, Oracle WebCenter Discussions Server, Oracle WebCenter Wiki and Blog Server, and so on.

### Audience

The content of this chapter is intended for Fusion Middleware administrators (users granted the `Admin` role through the Oracle WebLogic Server Administration Console) and WebCenter Spaces administrators (users granted the `WebCenter Spaces Administrator` role or a custom role that grants the `Application-Manage` permission).

See also, [Section 1.8, "Understanding Administrative Operations, Roles, and Tools"](#).

## 16.1 Exporting and Importing WebCenter Spaces for Data Migration

WebCenter Spaces provides a set of export and import utilities that enable you to back up or move content between WebCenter Spaces applications and stage or production environments. This section describes how to export and import the whole WebCenter Spaces application, as well as individual group spaces, and group space templates. It includes the following subsections:

- [Understanding WebCenter Spaces Export and Import](#)
- [Prerequisites for WebCenter Spaces Export and Import](#)

Migrating an entire WebCenter Spaces application:

- [Migrating Back-end Components for an Entire WebCenter Spaces Application](#)

- [Exporting an Entire WebCenter Spaces Application](#)
- [Importing an Entire WebCenter Spaces Application](#)

Migrating group spaces:

- [Prerequisites for Group Space Export and Import](#)
- [Migrating Back-end Components for Individual Group Spaces](#)
- [Exporting Group Spaces](#)
- [Importing Group Spaces](#)

Migrating group space templates:

- [Migrating Back-end Components for Group Space Templates](#)
- [Exporting Group Space Templates](#)
- [Importing Group Space Templates](#)

### 16.1.1 Understanding WebCenter Spaces Export and Import

Using export and import, Fusion Middleware administrators can migrate entire WebCenter Spaces applications between stage and production environments. This includes every personal space, group space, group space template, as well as application and service customizations (applied to the application, pages, and task flows), application and service metadata (object definitions), and data, as outlined in [Figure 16-1](#).

**Figure 16-1 Information Exported with WebCenter Spaces**

| Always Exported   | Export Optional   | Never Exported  |
|---|---|---|
| <p><b>MDS – Service Metadata</b></p> <ul style="list-style-type: none"> <li>● Announcements</li> <li>● Discussions</li> <li>● Group Space Events</li> <li>● Lists (Definitions)</li> <li>● Notes</li> <li>● Mail</li> <li>● Pages</li> <li>● Portlets</li> <li>● Recent Activities</li> <li>● Resource Catalog</li> <li>● RSS</li> <li>● Search</li> <li>● Tags</li> <li>● Worklists</li> </ul> <p><b>MDS – Service Data</b></p> <ul style="list-style-type: none"> <li>● Notes</li> </ul> <p><b>MDS – Customizations</b></p> <ul style="list-style-type: none"> <li>● Portlets</li> <li>● Pages</li> </ul> | <p><b>MDS - Customizations</b></p> <ul style="list-style-type: none"> <li>● Document Library Task Flow</li> <li>● Document List Viewer Task Flow</li> <li>● Lists Task Flow</li> <li>● Saved Searches Task Flow</li> <li>● WebCenter Spaces:                             <ul style="list-style-type: none"> <li>● WebCenter Administration</li> <li>● Group Space Settings</li> </ul> </li> </ul> <p><b>WebCenter Repository – Service Data</b></p> <ul style="list-style-type: none"> <li>● Group Space Events</li> <li>● Links</li> <li>● Lists</li> <li>● Tags</li> </ul> <p><b>Security Policy</b></p> <ul style="list-style-type: none"> <li>● policy-store.xml</li> </ul> | <p><b>MDS - Personalization</b></p> <ul style="list-style-type: none"> <li>● Pages</li> <li>● Task Flows</li> <li>● Application</li> </ul> <p><b>External – Service Interface</b></p> <ul style="list-style-type: none"> <li>● Documents</li> <li>● Announcements</li> <li>● Discussions</li> <li>● IMP</li> <li>● Mail</li> <li>● Wiki and Blog</li> <li>● Worklists</li> </ul> <p><b>Application Artefacts</b></p> <ul style="list-style-type: none"> <li>● Icons</li> <li>● Skins</li> <li>● Images</li> </ul> |



This migration can be performed using Fusion Middleware Control Console or WLST commands. For details, see:

- [Exporting WebCenter Spaces Using Oracle Enterprise Manager Fusion Middleware Control](#)
- [Exporting WebCenter Spaces Using WLST](#)
- [Importing WebCenter Spaces Using Oracle Enterprise Manager Fusion Middleware Control](#)
- [Importing WebCenter Spaces Using WLST](#)

### Group Space and Group Space Template Export and Import

WebCenter Spaces administrators can also export and import individual group spaces and group space templates, and their related objects, through WebCenter Spaces Administration and using WLST Commands.

The primary purpose of these export and import features is to enable cloning and migration of data. The export and import combination enables WebCenter Spaces administrators to:

- Move content between stage and production environments.
- Move content to remote instances.

For more detail, see.

- [Exporting Group Spaces](#)
- [Importing Group Spaces](#)
- [Exporting Group Space Templates](#)
- [Importing Group Space Templates](#)

### Customizations and Personalizations

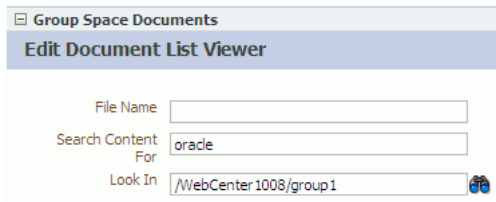
Some WebCenter Spaces customizations are optional on export, as noted in [Figure 16–1](#). For more information, see [Table 16–1](#) and [Table 16–2](#).

Personalizations made by users are not migrated during export and import. For more information on customization and personalization and the difference between them, see "Customizing and Personalizing Page Content" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

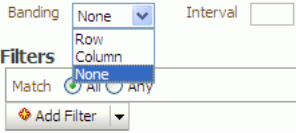
**Table 16–1 WebCenter Spaces - Service Customizations**

| Services in WebCenter Spaces       | Customizations | Export |
|------------------------------------|----------------|--------|
| <b>Announcements Service</b>       |                |        |
| Announcement Tab                   | None           |        |
| Announcement Task Flow             | None           |        |
| <b>Discussions Service</b>         |                |        |
| Sidebar                            | None           |        |
| Discussions Tab                    | None           |        |
| Discussion Forum Manager Task Flow | None           |        |
| Forum Task Flow                    | None           |        |
| Discussion Task Flows              | None           |        |

**Table 16–1 (Cont.) WebCenter Spaces - Service Customizations**

| Services in WebCenter Spaces                  | Customizations   | Export   |
|---|--|----------|
| <b>Documents Service</b>                      |  |          |
| Documents Tab                                 | None   |          |
| Document Library Task Flow                    | <ul style="list-style-type: none"> <li>Document Library display preferences, such as, Description, Size, Status, Modified by, Last Modified, Links, and so on.</li> <li>Table column settings, such as, visible columns, column sizes, and ordering.</li> </ul> <p>For information, see "What You Should Know About the Documents Service" in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter</i>.</p>   | Optional |
| Document List Viewer                          |  <p>Table column settings, such as, visible columns, column sizes, and ordering.</p> <p>In the page edit mode, default fields that display document search results can be customized and additional fields can be added.</p> <p>For information, see the section "Understanding the Personal and Group Space Documents Task Flows" in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter</i>.</p> | Optional |
| Recent Documents                              | None   |          |
| <b>Group Space Events Service</b>             |  |          |
| <b>Instant Messaging and Presence Service</b> |  |          |
| Buddies Task Flow                             | None   |          |
| <b>Lists Service</b>                          |  |          |
| List Tab                                      | None   |          |

**Table 16–1 (Cont.) WebCenter Spaces - Service Customizations**

| Services in WebCenter Spaces     | Customizations  | Export   |
|----------------------------------|---|----------|
| Lists Task Flow                  | Page edit mode: <ul style="list-style-type: none"> <li>Banding type and interval, and column filter settings</li> </ul>  <ul style="list-style-type: none"> <li>Column settings: Sort column and sort direction (ascending, descending), column sizes, and column order</li> </ul> <p>For information, see the section "Working with Lists Service Task Flows" in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter</i>.</p> | Optional |
| List Manager Task Flow           | None  |          |
| <b>Mail Service</b>              |   |          |
| Sidebar                          | None  |          |
| Mail Task Flow                   | None  |          |
| <b>Notes Service</b>             |   |          |
| <b>Pages</b>                     | Page edit mode: task flow and portlet customizations using Oracle Composer, such as, Maximize, Move, Vertical Height  | Always   |
|                                  | Page Properties: Page Name, Description, Keywords, Scheme, Scheme Background Color, Page Security, Page Parameters, Page modified date, and so on.  | Always   |
|                                  | Component Properties: Title, Background Color, and so on.   | Always   |
| <b>Portlets</b>                  | Customizations/edit defaults (if any) stored in producers.  | Always   |
| <b>Recent Activities Service</b> | None  |          |
| <b>Resource Catalog</b>          | None  |          |
| <b>RSS News Feed Service</b>     | None  |          |
| <b>Search Service</b>            | None  |          |
| Saved Search                     | Shared/Private option for saved searches. Saved search customizations.  | Optional |
| <b>Tags Service</b>              |   |          |
| Tags                             | None  |          |
| Tags Center                      | None  |          |
| Tag Sidebar                      | None  |          |
| <b>Worklist Service</b>          | None  |          |

**Table 16–2 WebCenter Spaces Application General Settings**

| WebCenter Spaces                | Customizations  | Export   |
|---------------------------------|---|----------|
| <b>Application Settings</b>     |   | Optional |
| Administration General tab      | All properties  |          |
| Administration Pages tab        | Settings such as, Set Page Defaults, Order, and Show Page               |          |
| Sidebar tab                     | All properties  |          |
| Discussions tab                 | All properties  |          |
| Profile tab                     | All properties  |          |
| Applications sidebar            | Applications/folders display order, and personalization allowed setting |          |
| Administration General tab      | Language  |          |
| <b>Group Space Settings</b>     |   | Optional |
| Group Spaces Settings Pages tab | Settings such as, Set Page Defaults, Order, and Show Page               |          |
| Other tabs                      | All properties  |          |

### 16.1.2 Prerequisites for WebCenter Spaces Export and Import

The Oracle Database in which the application metadata or schema is stored must be up and running for the successful completion of the export and import operation.

Some back-end components, specifically the Identity Store, Credential Store, and Policy Store, must be migrated before you export or import a WebCenter Spaces application. For more information, refer to the next section, [Section 16.1.3, "Migrating Back-end Components for an Entire WebCenter Spaces Application"](#).

WebCenter Spaces is temporarily unavailable during import and export operations to prevent data conflicts. Any user who tries to login or access WebCenter Spaces pages will see an "application unavailable" page.

### 16.1.3 Migrating Back-end Components for an Entire WebCenter Spaces Application

Before migrating a WebCenter Spaces application, you must migrate all the back-end components that are used by the application. This section tells you how.

The configured services in the target instance (the instance that is being imported into) must be a superset of what was configured in the instance that was exported. That is, the target must be configured with at least the same set of services that the source is configured with. If this is not the case, the import will fail.

The Identity Store, Credential Store, and Policy Store must be migrated *before* the application. The Oracle WebCenter Discussions Server, Oracle WebCenter Wiki Server, Oracle Content Server, Oracle WebLogic Communications Server, and portlet producers can be migrated after the WebCenter Spaces application, if preferred.

This section includes the following sub-sections:

- [Exporting the LDAP Identity Store](#)
- [Importing the LDAP Identity Store](#)
- [Exporting and Importing the LDAP Credential Store](#)
- [Exporting and Importing the LDAP Policy Store](#)

- [Exporting Oracle WebCenter Discussions Server](#)
- [Importing Oracle WebCenter Discussions Server](#)
- [Exporting Oracle WebCenter Wiki Server](#)
- [Importing Oracle WebCenter Wiki Server](#)
- [Exporting Oracle Content Server](#)
- [Importing Oracle Content Server](#)
- [Exporting Oracle WebLogic Communications Server](#)
- [Importing Oracle WebLogic Communications Server](#)
- [Exporting Portlet Producers](#)
- [Importing Portlet Producers](#)

### 16.1.3.1 Exporting the LDAP Identity Store

To export users, groups, and passwords from an *external* identity store, use the `ldapsearch` command. This command creates an `ldif` file, which the `ldapadd` command uses during the import operation. The `ldapsearch` utility is located in the OID/IdM `ORACLE_HOME/bin` directory.

[Example 16–1](#) shows the `ldapsearch` command for exporting an LDAP identity store. Where `LDAP_OH/bin` is the OID/IdM `ORACLE_HOME/bin` directory:

#### **Example 16–1** *ldapsearch Command to Export LDAP Identity Store*

```
LDAP_OH/bin/ldapsearch -h ldap_hostname -p ldap_port -D "cn=ldap_user" -w
password -b "cn=users,dc=example,dc=com"
-s subtree "objectclass=*" "*" orclguid -L > my_users.ldif
```

To migrate groups, repeat the command with appropriate group base DN. For example: `-b "cn=groups,dc=example,dc=com"`

For detailed syntax and examples, see "ldapsearch" and "ldapaddmt" in *Oracle Fusion Middleware User Reference for Oracle Identity Management*.

For information on migrating an external LDAP identity store, refer to "Managing Directory Entries" and "Performing Bulk Operations" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

---



---

**Note:** To migrate users, groups, and passwords between two *embedded* LDAP servers, refer to "Exporting and Importing Information in the Embedded LDAP Server" in *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

---



---

### 16.1.3.2 Importing the LDAP Identity Store

To import users and groups from another external identity store, use the `ldapaddmt` utility. The `ldapaddmt` utility is located in the OID/IdM `ORACLE_HOME/bin` directory.

[Example 16–2](#) shows how to run the `ldapaddmt` utility to import the `ldif` file. Where `LDAP_OH/bin` is the OID/IdM `ORACLE_HOME/bin` directory:

#### **Example 16–2** *ldapaddmt Utility to Import the Ldif File*

```
LDAP_OH/bin/ldapaddmt -h ldap_hostname -p ldap_port -D "cn=ldap_user" -w password
```

```
-c -r -f my_users.ldif
```

For detailed syntax and examples, see "ldapaddmt" in *Oracle Fusion Middleware User Reference for Oracle Identity Management*.

For information on migrating the LDAP identity store, refer to "Managing Directory Entries" and "Performing Bulk Operations" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

---



---

**Note:** To import users, groups, and passwords from another embedded LDAP server, refer to "Exporting and Importing Information in the Embedded LDAP Server" in *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

---



---

### 16.1.3.3 Exporting and Importing the LDAP Credential Store

To migrate your credential store to a different target, use the WLST command `migrateSecurityStore`. Before running this command you must specify details relating to your *source* credential store in a `jps-config.xml` file.

1. Create your own `jps-config.xml` (named `jps-config-cred.xml` in this example) and then specify the domain name, JPS root, and LDAP URL of the source credential store:

- a. Create a copy of your target's `jps-config.xml` file, located at `DOMAIN_HOME/config/fmwconfig/jps-config.xml`, and name the copy `jps-config-cred.xml` as follows:

```
cp MW_HOME/user_projects/domains/my_domain/config/fmwconfig/jps-config.xml
MW_HOME/user_projects/domains/my_
domain/config/fmwconfig/jps-config-cred.xml
```

- b. In the `jps-config-cred.xml` file, duplicate the following section:

```
<serviceInstance provider="ldap.credentialstore.provider"
name="credstore.ldap">
  ...
</serviceInstance>
```

The next few steps describes how to edit this new section to point to your *source* credential store. Once complete, `jps-config-cred.xml` file will contain both source and target information for the migration process.

- c. First, change the name of the new element to indicate that it contains *source* information. For example, change:

```
From: name="credstore.ldap."
To:   name="credstore.ldap.s"
```

- d. Modify the domain name, JPS root, and LDAP URL values as appropriate. For example:

```
<serviceInstance provider="ldap.credentialstore.provider"
name="credstore.ldap.s">
  <property value="bootstrap"
name="bootstrap.security.principal.key"/>
  <property value="cn=my_domain"
name="oracle.security.jps.farm.name"/>
  <property value="cn=jpsroot_webcenter_mytest_to_prod"
name="oracle.security.jps.ldap.root.name"/>
```

```
<property value="ldap:myhost:myport" name="ldap.url"/>
</serviceInstance>
```

- e. Since we're only concerned with the credential store, modify the `<jpsContext name="default">` element, removing references to the identity store and the policy store. For example:

```
<jpsContext name="default">
  <serviceInstanceRef ref="keystore"/>
  <serviceInstanceRef ref="audit"/>
  <serviceInstanceRef ref="credstore.ldap"/>
</jpsContext>
```

- f. Duplicate the `<jpsContext>` element, and change the name in the new `<jpsContext>` element to "source". For example, change:

From: `<jpsContext name="default">`

To: `<jpsContext name="source">`

- g. Modify the credential store reference to point to the value specified in step c. For example:

```
<jpsContext name="source">
  <serviceInstanceRef ref="keystore"/>
  <serviceInstanceRef ref="audit"/>
  <serviceInstanceRef ref="credstore.ldap.s"/>
</jpsContext>
```

2. Find the name of the source folder using the `ldapsearch` utility.

For example, enter:

```
LDAP_OH/bin/ldapsearch -h srcldap_hostname -p ldap_port -D "cn=ldap_user" -w
password -b "" -s sub "cn=<application_name>-*"
```

Where `<application_name>` is the name of the source WebCenter application.

The folder name returned is named: `<application_name>-xxxx`

For WebCenter Spaces, `<application_name>` is always `webcenter`. If, for example, the source folder is named `webcenter-1646`, the following information might be returned:

```
cn=webcenter-1646,cn=CredentialStore,cn=my_domain, cn=JPSContext, cn=jpsroot_
webcenter_t2ptest
objectclass=top
objectclass=orclContainer
cn=webcenter-1646
```

3. Find the name of the destination folder using the `ldapsearch` utility.

For example, enter:

```
LDAP_OH/bin/ldapsearch -h dstldap_hostname -p ldap_port -D "cn=ldap_user" -w
password -b "" -s sub "cn=<application_name>-*"
```

Where `<application_name>` is the name of the destination WebCenter application.

The folder name returned is named: `<application_name>-xxxx`

For WebCenter Spaces, `<application_name>` is always `webcenter`.

4. To import the credential store, run the WLST command `migrateSecurityStore`.

For example (Example 16-3):

**Example 16-3 migrateSecurityStore - Credential Store**

```
migrateSecurityStore(type="credStore", configFile="/MW_HOME/user_
projects/domains/my_domain/config/fmwconfig/jps-config-cred.xml",
src="source", dst="default", overwrite="true", srcFolder="<source folder>",
dstFolder="<destination folder>")
```

For detailed syntax and examples, see "migrateSecurityStore" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

### 16.1.3.4 Exporting and Importing the LDAP Policy Store

With WebCenter Spaces, there is no need for manual policy store migration because the WebCenter Spaces export/import commands migrate security policy data for you. For details, see [Section 16.1.4, "Exporting an Entire WebCenter Spaces Application"](#).

While Oracle does not recommend that you perform policy store migration manually for WebCenter Spaces, there may be circumstances where this is required. In such cases, use the WLST command `migrateSecurityStore` to perform the migration as described below.

For custom WebCenter applications, always use the `migrateSecurityStore` command to migrate security policy data.

Before running the `migrateSecurityStore` command you must specify details relating to your *source* policy store in a `jps-config.xml` file.

1. Create your own `jps-config.xml` (named `jps-config-policy.xml` in this example) and then specify the domain name, JPS root, and LDAP URL of the source policy store:

- a. Create a copy of your target's `jps-config.xml` file, located at `DOMAIN_HOME/config/fmwconfig/jps-config.xml`, and name the copy `jps-config-policy.xml` as follows:

```
cp MW_HOME/user_projects/domains/my_domain/config/fmwconfig/jps-config.xml
MW_HOME/user_projects/domains/my_
domain/config/fmwconfig/jps-config-policy.xml
```

- b. In the `jps-config-policy.xml` file, duplicate the following section:

```
<serviceInstance provider="ldap.policystore.provider"
name="policystore.ldap">
...
</serviceInstance>
```

The next few steps describes how to edit this new section to point to your *source* policy store. Once complete, `jps-config-policy.xml` file will contain both source and target information for the migration process.

- c. First, change the name of the new element to indicate that it contains *source* information. For example, change:

From: `name="policystore.ldap."`

To: `name="policystore.ldap.s"`



- d. Modify the domain name, JPS root, and LDAP URL values as appropriate. For example:

```
<serviceInstance provider="ldap.policytore.provider"
name="policystore.ldap.s">
    <property value="bootstrap"
name="bootstrap.security.principal.key"/>
    <property value="cn=my_domain"
name="oracle.security.jps.farm.name"/>
    <property value="cn=jpsroot_webcenter_mytest_to_prod"
name="oracle.security.jps.ldap.root.name"/>
    <property value="ldap:myhost:myport" name="ldap.url"/>
</serviceInstance>
```

- e. Duplicate the `<jpsContext>` element, and change the name in the new `<jpsContext>` element to "source". For example, change:

From: `<jpsContext name="default">`

To: `<jpsContext name="source">`

- f. Modify the policy store reference to point to the value specified in step c, removing references to the identity store and the credential store. For example:

```
<jpsContext name="source">
    <serviceInstanceRef ref="keystore"/>
    <serviceInstanceRef ref="audit"/>
    <serviceInstanceRef ref="policystore.ldap.s"/>
</jpsContext>
```

- g. Modify the `<jpsContext name="default">` element, removing references to the identity store and the credential store. For example:

```
<jpsContext name="default">
    <serviceInstanceRef ref="keystore"/>
    <serviceInstanceRef ref="audit"/>
    <serviceInstanceRef ref="policystore.ldap"/>
</jpsContext>
```

2. Find the full name of the source WebCenter application using the `ldapsearch` utility.

For example, enter:

```
LDAP_OH/bin/ldapsearch -h srcldap_hostname -p srcldap_port -D "cn=ldap_user"
-w password -b "" -s sub "orclapplicationcommonname=<application_name>*"
```

Where `<application_name>` is the name of the source WebCenter application.

The application name returned is: `<application_name>xxxxx`

For WebCenter Spaces, `<application_name>` is always `webcenter`. If, for example, the full source application name is `webcenter#V2.0`, the following information might be returned:

```
cn=webcenter\#V2.0,cn=my_domain,cn=JPSContext,cn=jpsroot_webcenter_t2ptest
objectclass=top
objectclass=orclJavaApplicationEntity
orclapplicationcommonname=webcenter#V2.0
cn=webcenter#V2.0
```

3. Find the full name of the destination WebCenter application using the `ldapsearch` utility.

For example, enter:

```
LDAP_OH/bin/ldapsearch -h dstldap_hostname -p dstldap_port -D "cn=ldap_user"
-w password -b "" -s sub "orclapplicationcommonname=<application_name>*"
```

Where <application\_name> is the name of the destination WebCenter application.

The application name returned is: <application\_name>xxxxx

For WebCenter Spaces, <application\_name> is always webcenter.

4. To import the policy store, run the WLST command `migrateSecurityStore`.

For example (Example 16-4):

#### **Example 16-4 migrateSecurityStore - Policy Store**

```
migrateSecurityStore(type="appPolicies", configFile="/MW_HOME/user_
projects/domains/my_domain/config/fmwconfig/jps-config-policy.xml",
src="source",dst="default",overwrite="true", srcApp="<full application name>",
dstApp="<full application name>")
```

For detailed syntax and examples, see "migrateSecurityStore" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

### **16.1.3.5 Exporting Oracle WebCenter Discussions Server**

To export Oracle WebCenter Discussions Server, use the database export utility. For example, go to `ORACLE_HOME/bin` of your database and run the command described in Example 16-5.

---



---

**Note:** The Oracle Data Pump utility does not support LONG columns types that exist in the DISCUSSIONS schema. Therefore Oracle recommends using Oracle Database Utilities. See also, *Oracle Database Utilities*.

---



---

#### **Example 16-5 Export Database Utility**

```
DB_OH/bin/exp \"sys/password@dbhost serviceid as sysdba\" OWNER=rcuprefix_
DISCUSSIONS FILE=/tmp/df.dmp STATISTICS=none
```

where:

- `DB_OH` is the directory in which database for Oracle WebCenter Discussions Server schema is installed.
- `password` is the password for the system database user.
- `dbhost` is the SID or TNS entry for the database
- `OWNER` is the schema to be exported. This is the RCU suffix that was used during installation, `_DISCUSSIONS`, along with the user supplied prefix. For example, `DEV_DISCUSSIONS`.
- `FILE` contains the exported data.

### **16.1.3.6 Importing Oracle WebCenter Discussions Server**

To import Oracle WebCenter Discussions Server, use the database import utility.

---



---

**Note:** The Oracle Data Pump utility does not support LONG columns types that exist in the DISCUSSIONS schema. Therefore Oracle recommends using Oracle Database Utilities. See also, *Oracle Database Utilities*.

---



---

1. Shut down the target Oracle WebCenter Discussions Server.
2. Go to `ORACLE_HOME/bin` of your database where Oracle WebCenter Discussions Server schema is installed, and connect to the database using the `sqlplus` as `sysadmin`:  

```
DB_OH/bin/sqlplus "sys/password@dbhost as sysdba"
```
3. Drop the target user:  

```
drop user tgtrcuprefix_DISCUSSIONS cascade;
```
4. Create the target user:  

```
create user tgtrcuprefix_DISCUSSIONS identified by password default tablespace tgtrcuprefix_DISCUSSIONS temporary tablespace name_IAS_TEMP;
```
5. Grant connect and resource to the user:  

```
grant connect,resource to tgtrcuprefix_DISCUSSIONS;
```
6. Exit `sqlplus`.
7. Run the import tool as described in [Example 16–6](#).

#### **Example 16–6 Database Import Utility**

```
DB_OH/bin/imp \"sys/password@dbhost as sysdba\" FROMUSER=srcrcuprefix_DISCUSSIONS TOUSER=tgtrcuprefix_DISCUSSIONS FILE=/tmp/df.dmp statistics=none
```

where:

- `DB_OH` is the directory in which database for Oracle WebCenter Discussions Server schema is installed.
- `password` is the password for the system database user.
- `dbhost` is the host name of the database.
- `FROMUSER` is the exported schema.
- `TOUSER` is the imported schema. This is the RCU suffix that was used during installation, `_DISCUSSIONS`, along with the user supplied prefix. For example, `DEV_DISCUSSIONS`.
- `FILE` contains the data to be imported.

#### **16.1.3.7 Exporting Oracle WebCenter Wiki Server**

To export Oracle WebCenter Wiki Server, use the Data Pump export utility. For example, go to `ORACLE_HOME/bin` of your database and run the command described in [Example 16–7](#).

**See Also:** For more information, see "Oracle Data Pump" in *Oracle Database Utilities*.

**Example 16–7 Data Pump Export Utility**

```
DB_OH/bin/exp \"sys/password@dbhost as sysdba\" OWNER=rcuprefix_WIKI
FILE=/tmp/wiki.dmp STATISTICS=none
```

where:

- DB\_OH is the directory in which database for Oracle WebCenter Wiki Server schema is installed.
- password is the password for the system database user.
- dbhost is the host name of the database.
- OWNER is the schema to be exported. This is the RCU suffix that was used during installation, \_WIKI, along with the user supplied prefix. For example, DEV\_WIKI.
- FILE contains the exported data.

**16.1.3.8 Importing Oracle WebCenter Wiki Server**

To import Oracle WebCenter Wiki Server, use the Oracle Data Pump import utility.

---



---

**Note:** The Oracle Data Pump utility does not support LONG columns types that exist in the WIKI schema. Therefore Oracle recommends using Oracle Database Utilities. See also, *Oracle Database Utilities*.

---



---

1. Shut down the target Oracle WebCenter Wiki Server.
2. Go to `ORACLE_HOME/bin` of your database where the Oracle WebCenter Wiki Server schema is installed, and connect to the database using the sqlplus as sysadmin:

```
DB_OH/bin/sqlplus "sys/password@dbhost as sysdba"
```

3. Drop the target user:

```
drop user tgtrcuprefix_WIKI cascade;
```

4. Create the target user:

```
create user tgtrcuprefix_WIKI identified by password default tablespace
tgtrcuprefix_WIKI temporary tablespace name_TEMP;
```

5. Grant connect and resource to the user:

```
grant connect,resource to tgtrcuprefix_WIKI;
```

6. Exit sqlplus.

7. Run the import tool as described in [Example 16–8](#).

**Example 16–8 Database Import Utility**

```
DB_OH/bin/imp \"sys/password@dbhost as sysdba\" FROMUSER=srcrcuprefix_WIKI
TOUSER=tgtrcuprefix_WIKI FILE=/tmp/wiki.dmp statistics=none
```

where:

- DB\_OH is the directory in which database for Oracle WebCenter Wiki Server schema is installed.

- password is the password for the system database user.
- dbhost is the host name of the database.
- FROMUSER is the exported schema.
- TOUSER is the imported schema. This is the RCU suffix that was used during installation, \_WIKI, along with the user supplied prefix. For example, DEV\_WIKI.
- FILE contains the data to be imported.

### 16.1.3.9 Exporting Oracle Content Server

To export Oracle Content Server, use the Oracle Data Pump export utility. For example, go to `ORACLE_HOME/bin` of your database and run the command described in [Example 16-9](#).

**See Also:** For more information, see "Oracle Data Pump" in *Oracle Database Utilities*.

#### Example 16-9 Data Pump Utility (Export)

```
DB_OH/bin/expdp \"sys/password@dbhost as sysdba\" SCHEMAS=srcrcuprefix_OCSEVER
DIRECTORY=data_pump_dir DUMPFILE=UCM.dmp
```

where:

- DB\_OH is the directory in which database for Oracle Content Server schema is installed.
- password is the password for system database user.
- dbhost is the host name of the database.
- SCHEMAS is the schema of the database. This is the RCU suffix that was used during installation, \_OCSEVER, along with the user supplied prefix. For example, DEV\_OCSEVER.
- DIRECTORY specifies the directory object created for the export and import operation.

---

**Note:** The `data_pump_dir` file must have been created in SQL using a tool like SQL\*Plus. For example:

```
SQL> create or replace directory DATA_PUMP_DIR as '<full_path_to_a_
directory_on_the_file_system>';
SQL> commit;
SQL> quit
```

---

- DUMPFILE contains the exported data. This file is used during import.

### 16.1.3.10 Importing Oracle Content Server

To import Oracle Content Server, use the Oracle Data Pump import utility. For example, go to `ORACLE_HOME/bin` of your database and run the command described in [Example 16-10](#).

**See Also:** For more information, see "Oracle Data Pump" in *Oracle Database Utilities*.

**Example 16–10 Data Pump Utility (Import)**

```
DB_OH/bin/impdp \ "sys/password@dbhost as sysdba\" REMAP_SCHEMA=srscuprefix_  
OCSEVER:tgtrcuprefix_OCSEVER  
DIRECTORY=data_pump_dir DUMPFILE=UCM.dmp TABLE_EXISTS_ACTION=REPLACE
```

where:

- DB\_OH is the directory in which database for Oracle Content Server schema is installed.
- password is the password for system database user.
- dbhost is the host name of the database.
- REMAP\_SCHEMA maps the schema exported from the stage environment to the schema in the production environment. This is the RCU suffix that was used during installation, \_OCSEVER, along with the user supplied prefix. For example, DEV\_OCSEVER.
- DIRECTORY specifies the directory object created for the export and import operation.

---

---

**Note:** The data\_pump\_dir file must have been created in SQL using a tool like SQL\*Plus. For example:

```
SQL> create or replace directory DATA_PUMP_DIR as '<full_path_to_a_  
directory_on_the_file_system>';  
SQL> commit;  
SQL> quit
```

---

---

- DUMPFILE contains the data to be imported.
- TABLE\_EXISTS\_ACTION replaces the existing table with the imported table.

After the Oracle Content Server repository has been imported, log into WebCenter Spaces and ensure that the Documents service is provisioned for that Group Space. The provisioned/unprovisioned state of Documents in a group space is determined by the presence of a group space specific folder in the Content Server. This occurs when the you provision the group space for a new Content Server instance, or when the already provisioned source Content Server is exported and imported to the target Content Server.

**16.1.3.11 Exporting Oracle WebLogic Communications Server**

For information on exporting Oracle WebLogic Communications Server, see *Oracle WebLogic Communication Services Administrator's Guide*.

**16.1.3.12 Importing Oracle WebLogic Communications Server**

For information on importing Oracle WebLogic Communications Server, see *Oracle WebLogic Communication Services Administrator's Guide*.

**16.1.3.13 Exporting Portlet Producers**

This step is only required if you want to migrate entire producer metadata and not just the producer metadata associated with your WebCenter Spaces application. For information on how to export entire producer metadata, see the appendix "Portlet Preference Store Migration Utilities" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

### 16.1.3.14 Importing Portlet Producers

This step is only required if you want to migrate entire producer metadata and not just the producer metadata associated with your WebCenter Spaces application. For information on how to import entire producer metadata, see the appendix "Portlet Preference Store Migration Utilities" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

## 16.1.4 Exporting an Entire WebCenter Spaces Application

This section describes how to export an entire WebCenter Spaces application using Oracle Enterprise Manager Fusion Middleware Control and WLST commands.

A WebCenter Spaces application is exported into a single export archive (.ear file). The EAR file contains a metadata archive (.mar file) and a single XML file containing the security policy information. You can save export archives to your local file system or to a remote server file system. For more information about what is exported, read [Section 16.1.1, "Understanding WebCenter Spaces Export and Import"](#).

WebCenter Spaces is temporarily unavailable during import and export operations to prevent data conflicts. Any user who tries to login or access WebCenter Spaces pages will see an "application unavailable" page.

The export process does not include data associated with external services, that is, Mail, Discussions, Announcements, Worklists, Wiki, Blogs, Instant Messaging and Presence (IMP), and Documents. To learn how to move data associated with these services, see [Section 16.1.3, "Migrating Back-end Components for an Entire WebCenter Spaces Application"](#).

If a shared identity store is not used and the users in both the export and import environment must be identical, then these users must also be migrated. Refer to [Section 16.1.3, "Migrating Back-end Components for an Entire WebCenter Spaces Application"](#).

---

**Note:** No icons, skins, images, or personalizations are exported. For information on personalizations, see the section "Personalizing Your Page View" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

---

This section includes the following:

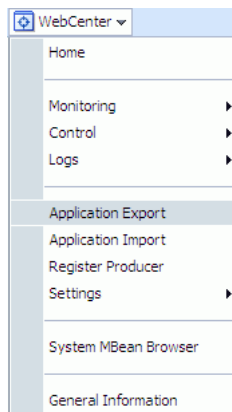
- [Exporting WebCenter Spaces Using Oracle Enterprise Manager Fusion Middleware Control](#)
- [Exporting WebCenter Spaces Using WLST](#)

### 16.1.4.1 Exporting WebCenter Spaces Using Oracle Enterprise Manager Fusion Middleware Control

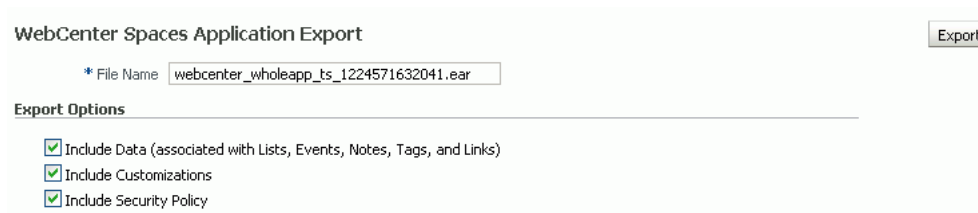
Fusion Middleware administrators can export an entire WebCenter application using Fusion Middleware Control.

To export WebCenter Spaces:

1. In Fusion Middleware Control, navigate to the home page for WebCenter Spaces. See [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#).
2. From the **WebCenter** menu, select **Application Export**, as shown in [Figure 16–2](#).

**Figure 16–2 WebCenter Menu - Application Export Option**

3. Change the **File Name** for the export archive or accept the default name.  
To ensure uniqueness, the default `.ear` filename contains a timestamp:  
`webcenter_wholeapp_ts_timestamp.ear`, as shown in [Figure 16–3](#).

**Figure 16–3 Select the Archive to be Exported**

4. Set export options as required. For details, see [Table 16–3](#).

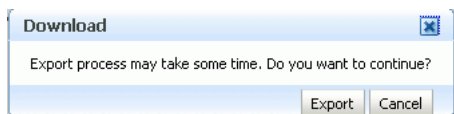


**Table 16–3 WebCenter Spaces Application Export Options**

| Field                   | Description  |
|-------------------------|--|
| Include Data            | <p>Select to export data stored in the WebCenter repository for Lists, Events, Links, and Tags. For example, list items, group space events, any links/associations between objects in the application, and tag data. Note data stored in the MDS repository is exported too.</p> <p>Always re-export list data if source and target list definitions do not match. Mis-match only occurs when a list definition exists on the target and it is subsequently changed in the source.</p> <p>If the application selected for export contain a large amount of data, consider using the database export utilities to export the WebCenter schema data instead. For example:</p> <pre>DB_OH/bin/expdp \<code>"sys/password@dbhost as sysdba"</code> schemas=RCUPREFIX_WEBCENTER directory=data_pump_dir dumpfile=WC.dmp</pre> <p>For details, refer to <i>Oracle Database Utilities</i>.</p> <p>Deselect this option if you do not want to export any data associated with lists, events, tags, and links. For example, when moving an application from a test environment to a stage or production environment the test data may no longer be required.</p> <p><b>Note:</b> The export process does <i>not</i> export data associated with other, external services such as Mail, Discussions, Announcements, Worklists, Instant Messaging and Presence (IMP), and Documents. To learn how to move data associated with these services, see documentation for that product. See also, <a href="#">Section 16.1.3, "Migrating Back-end Components for an Entire WebCenter Spaces Application"</a>.</p> |
| Include Customizations  | <p>Select to export application customizations. For information about which customizations are optional on export, see <a href="#">Table 16–1</a> and <a href="#">Table 16–2</a>.</p> <p>If you deselect this option, WebCenter Spaces is exported without these application customizations.</p> <p>Portlet and page customizations are always exported. See also <a href="#">Figure 16–1, "Information Exported with WebCenter Spaces"</a>.</p>   |
| Include Security Policy | <p>Select to generate an XML file (<code>policy-store.xml</code>) listing:</p> <ul style="list-style-type: none"> <li>■ WebCenter Spaces application roles (and permissions assigned to each role).</li> <li>■ WebCenter user role assignments.</li> <li>■ Group space members (and their role assignments).</li> </ul> <p>Deselect this option if you do not want to export user details, that is, users and their current role assignments. When you import an application without user data, the WebCenter Spaces administrator that is importing the application becomes the default moderator for any group spaces that are imported. This option is useful when exporting applications between a stage and production environments where users used during testing are no longer required.</p>   |

**5. Click Export.**

- 6. In the Download dialog, as shown in [Figure 16–3](#), click **Export** to confirm that you want to go ahead.**

**Figure 16–4 Download**

Progress information is displayed during the export process. The application being exported cannot be accessed during export operations.

7. When the export process is complete, specify a location for the export archive (.ear). Select one of:
  - **Download** - Saves the export EAR file to your local file system.  
Your Browser will download and save the archive locally. The actual download location depends on your Browser set up.
  - **Save to Server** - Saves the export EAR file to a server location. For example, /tmp. Ensure that the server directory you specify has write permissions.  
After clicking **Save to Server**, enter the **Server Location** and then click **Save**.
8. Click **Close** to dismiss the Export window.

The export archive (.EAR) is saved to the specified location.

Check the diagnostic log file, `WLS_Spaces-diagnostics.log`, for warnings or errors during the export process. For details, see [Section 15.3, "Viewing and Configuring Log Information"](#). See also [Appendix B, "Troubleshooting"](#).

#### 16.1.4.2 Exporting WebCenter Spaces Using WLST

Use the WLST command `exportWebCenterApplication` to export WebCenter Spaces. For command syntax and examples, see "exportWebCenterApplication" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands"](#).

---



---

**Note:** No icons, skins, images, or personalizations are exported. For information on personalizations, see the section "Personalizing Your Page View" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

---



---

### 16.1.5 Importing an Entire WebCenter Spaces Application

This section describes how to import an entire WebCenter Spaces application using Fusion Middleware Control and WLST commands.

Before importing WebCenter Spaces:

- Migrate the LDAP Identity Store, Credential Store, Oracle WebCenter Discussions Server, and Oracle WebCenter Wiki. See [Section 16.1.3, "Migrating Back-end Components for an Entire WebCenter Spaces Application"](#).
- Oracle also recommends that you backup the WebCenter repository, MDS, and your policy store. See [Section 16.3, "Backing Up and Recovering WebCenter Applications"](#).
- Check that all users assigned to the `Administrator` role exist in the target identity store. On import, users listed in the WebCenter Spaces security policy are

checked against the identity store that is configured for the domain. If a user is not found, any policies associated with that user are removed. See also, [Section 14.3.4, "Moving the Administrator Account to an External LDAP Server"](#).

WebCenter Spaces is temporarily unavailable during import and export operations to prevent data conflicts. Any user who tries to login or access WebCenter Spaces pages will see an "application unavailable" page.

This section includes the following:

- [Importing WebCenter Spaces Using Oracle Enterprise Manager Fusion Middleware Control](#)
- [Importing WebCenter Spaces Using WLST](#)

### 16.1.5.1 Importing WebCenter Spaces Using Oracle Enterprise Manager Fusion Middleware Control

Fusion Middleware administrators can import an entire WebCenter application using Fusion Middleware Control.

To import a WebCenter Spaces application using Fusion Middleware Control:

1. In Fusion Middleware Control, navigate to the home page for WebCenter Spaces. See [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#).
2. From the **WebCenter** menu, select **Application Import**.
3. In the WebCenter Spaces Application Import page, as shown in [Figure 16–5](#), specify the location of your WebCenter Spaces application archive (.ear). Select one of the following:
  - **Archive Located on Local File System** - Enter the **File System Location**. Alternatively, click **Browse** to locate the directory on the local file system where the .ear file is stored.
  - **Archive Located on Server File System** - Enter the **Server Location**. Any shared location accessible from this WebCenter Spaces application.

**Figure 16–5 WebCenter Spaces Application Import Page**

4. Click **Import**.
5. In the WebCenter Spaces Application Import dialog, as shown in [Figure 16–6](#), click **Import**.

**Figure 16–6 WebCenter Spaces Application Import dialog**

Once the import is complete, a success message displays.

- Restart the managed server on which the newly imported WebCenter Spaces application is deployed.

In a cluster environment, restart each managed server in the cluster. See also, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments"](#).

### 16.1.5.2 Importing WebCenter Spaces Using WLST

Use the WLST command `importWebCenterApplication` to import a WebCenter Spaces. For command syntax and examples, see "importWebCenterApplication" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

If you intend to import group spaces with names identical to those available on the target application, ensure that group spaces in the target application are offline. If existing group spaces with identical names are online, then the import fails.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands"](#).

---

---

**Note:** After import, restart the managed server on which the newly imported WebCenter Spaces application is deployed. In a cluster environment, restart each managed server in the cluster. See also, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments"](#).

---

---

## 16.1.6 Prerequisites for Group Space Export and Import

To export one or more group spaces, the WebCenter Spaces application which contains the group spaces must be up and running, and all the group spaces you want to export must be offline to prevent data conflicts. See, [Section 22.3.1, "Taking Any Group Space Offline"](#).

Some back-end components, specifically Oracle WebCenter Discussions Server and Oracle WebCenter Wiki Server, must be migrated before you export or import group spaces. See next section, [Section 16.1.7, "Migrating Back-end Components for Individual Group Spaces"](#).

---

---

**Note:** The simultaneous export or import of large numbers of group spaces is not recommended as, depending on server configuration, it may affect system performance. If a serious deterioration in performance is observed, break the export or import down into smaller chunks.

---

---

## 16.1.7 Migrating Back-end Components for Individual Group Spaces

When migrating one or more group spaces, you must also migrate the back-end components used by the group space. This section tells you how.

This section includes the following sub sections:

- [Exporting Discussions for a Group Space](#)
- [Importing Discussions for a Group Space](#)
- [Exporting Wikis and Blogs for a Group Space](#)
- [Importing Wikis and Blogs for a Group Space](#)

- [Exporting Documents for a Group Space](#)
- [Importing Documents for a Group Space](#)

You must import the group spaces on to the target *before* importing these back-end components.

### 16.1.7.1 Exporting Discussions for a Group Space

Use the Oracle WebCenter Discussions Server Admin Console to export discussions associated with a particular group space.

Group space discussions are exported to an `.xml` file, and saved to a `.zip` file in the `DOMAIN_HOME/fmwconfig/server/<target_server_name>/owc_discussions_11.1.1.1.0/data` directory.

Where `DOMAIN_HOME` is the path to the Oracle WebLogic Server domain. For example, `MW_HOME/user_projects/domains/my_domain/fmwconfig/server/WLS_Services/owc_discussions_11.1.1.1.0/data`.

Before importing group space discussions on the target system, the target group space must exist. See [Section 16.1.9.1, "Importing Group Spaces Using WebCenter Spaces"](#).

To export group space discussions:

1. Login to the Oracle WebCenter Discussions Server Admin Console.

You can login directly if you know the console's URL. For example:  
`http://example.com:8890/owc_discussions/admin`

Alternatively, login through WebCenter Spaces as follows:

- a. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator."](#)
- b. Click the **Administration** link at the top of the application.
- c. Click the **Group Spaces** tab.
- d. From the **Actions** menu, choose **Edit Group Space**, for the group space you want to export.
- e. Click the **Services** tab, then **Discussions**.
- f. Note down the **Forum Name/ID** or **Category Name/ID** associated with this group space.

Oracle WebCenter Discussions Server generates discussion category and forum IDs sequentially. If this ID exists on the target system, the imported forum (or category) will be assigned a new, unique ID, and therefore you must reconfigure the imported group space, to point to the new ID. For details, see [Section 16.1.9.1, "Importing Group Spaces Using WebCenter Spaces"](#) - Step 11.

- g. Click **Forum Administration**, and login to the Admin Console.
2. In the Admin Console, select the **System** menu and choose **XML Export & Import** in the sidebar.
3. Select **Data Export**.
4. Set the following options ([Figure 16-7](#)):
  - a. **Export Options** - Select **Custom Options**, and select all the check boxes.
  - b. **Export Content** - Select **Export Specific Content**, and select the name of the forum or category required.

Note: Group spaces that support multiple forums will use a category to store discussions. Other group spaces use a single forum.

- c. **Export location, Export filename, Export file encoding** - Keep the default values.

**Figure 16–7 Exporting Group Space Discussions**

The screenshot shows the 'XML Export' configuration page in the Jive Forums Admin Console. The page is titled 'XML Export' and includes a warning: 'Use the options below to export data from the system. Note, exporting data from your system will likely cause a lot of database load and \M activity. Because of this, its best to export data at off-peak hours.'

**Export Options:**

- Standard Options - All users, groups, permissions are exported.
- Custom Options - Pick what to export:
  - Export global properties
  - Export users
  - Export groups
  - Export permissions
  - Export Attachments

**Export Content:**

- Export all content
- Export no content
- Export specific content:
  - Forums:**
    - qsp0
    - qsp0-Announcements
    - group1-Announcements
  - Categories:**
    - WebCenter
    - WebCenter + FinanceProject

Export private messages

**Export Location:**

- Save file to jiveHome data dir: oracle/product/jive/jive\_forums\_silver\_5\_5\_20\_oracle/jiveHome/data
- Send output to browser

**Export Filename:**

- Standard Filename: 2009-04-22-0330.xml (date stamp filename)
- Custom Filename:

**Export File Encoding:**

- System default encoding (UTF-8)
- Unicode (UTF-8)
- Pick a supported encoding:
  - UTF-8

5. Click **Start Export**.
6. Once complete, copy the .zip file (that contains the export .xml file) from the MW\_HOME/user\_projects/domains/my\_domain/fmwconfig/server/<server\_name>/owc\_discussions\_11.1.1.1.0/data directory to same location on the target discussions server. For example, MW\_HOME/user\_projects/domains/my\_domain/fmwconfig/server/WLS\_Services/owc\_discussions\_11.1.1.1.0/data.

Before importing group space discussions on the target system, the group space you are migrating must exist on the target. See [Section 16.1.9.1, "Importing Group Spaces Using WebCenter Spaces"](#).

### 16.1.7.2 Importing Discussions for a Group Space

Use the Oracle WebCenter Discussions Server Admin Console to import group space discussions exported from another WebCenter Spaces application.

Ensure that the associated group space exists on the target before you import the group space discussion data. See [Section 16.1.8.1, "Exporting Group Spaces Using WebCenter Spaces"](#).

---

**Note:** Oracle WebCenter Discussions Server generates discussion category and forum IDs sequentially. Therefore, when importing discussion data between two targets (or source to target), there is a chance that the same IDs will exist on both systems. When ID clashes occur, the imported forum (or category) is assigned a new, unique ID and as a result you must reconfigure the group space to point to the new ID. See Step 11 below for details.

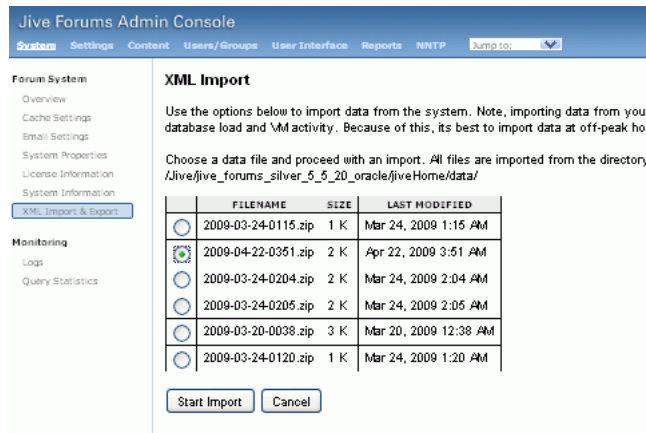
---

To import group space discussions:

1. Login to the Oracle WebCenter Discussions Server Admin Console.  
You can login directly if you know the console's URL. For example:  
`http://example.com:8890/owc_discussions/admin`  
Alternatively, login through WebCenter Spaces as follows:
  - a. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator."](#)
  - b. Click the **Administration** link at the top of the application.
  - c. Click the **Group Spaces** tab.
  - d. From the **Actions** menu, choose **Edit Group Space**, for the group space you want to export.
  - e. Click the **Service** tab, then **Discussions**.
  - f. Click **Forum Administration**, and login to the Admin Console.
2. In the Admin Console, select the **System** menu and then choose **XML Export & Import** in the sidebar.
3. Select **Data Import**.
4. Choose the appropriate group space export file from the list available ([Figure 16-8](#)).

If the file you want is not listed, copy the export .zip file from the source directory `DOMAIN_HOME/fmwconfig/server/<target_server_name>/owc_discussions_11.1.1.1.0/data` to same location on this target. See also, [Section 16.1.7.1, "Exporting Discussions for a Group Space"](#).

Where `DOMAIN_HOME` is the path to the Oracle WebLogic Server domain. For example, `MW_HOME/user_projects/domains/my_domain/fmwconfig/server/WLS_Services/owc_discussions_11.1.1.1.0/data`.

**Figure 16–8 Importing Group Space Discussions**

5. Click **Start Import**.

On import, the group space discussions data is copied to the discussions server. In the next step you will reassociate the group space you migrated earlier with this newly imported data.

6. Select the **Content** menu, and then choose **Content Summary** in the sidebar.

All the categories and forums in the system are listed here.

7. Select **WebCenter**, and then click the **Move** button for the newly imported forum or category.

8. Select the root category for the target WebCenter Spaces application, and click **Move Categories**.

The Category Summary page shows the new location.

9. Click **Permissions** in the sidebar.

10. Deselect all the permissions for the User Types: **Anyone** and **Registered Users**, and click **Save Changes** (Figure 16–9).



Figure 16–9 Editing Forum Permissions

**Jive Forums Admin Console** Jive Forums Silver 5.5.20 -oracle  
System Settings Content Users/Groups User Interface Reports NNTP Jump to: Logout [admin]

**Categories & Forums**  
Category Summary  
Category Options  
Category Settings  
Admins/Moderators  
Permissions  
Extended Properties  
Message Filters

**Moderation**  
Moderation Settings  
Moderation Summary  
Avatar Moderation

**Global Settings**  
Message Filters  
Autosave Settings

**Forum Category Permissions** Main » Categories & Forums » Forum Category Permissions

**Category List » Philatelists**  
Edit category permissions to set the permissions policies that the category will use.

Permissions are either additive or negative. Additive permissions (  ) are permissions that should be 'added' to the permissions retrieved from parent categories and those that are globally set, while negative permissions (  ) are permissions that should be revoked or removed from permissions retrieved from parent categories and those that are globally set. For more information about permissions, please read the administrator guide distributed with this product or click the help icon above.

**Note:** Checkboxes on this page have three states (    ). Click a checkbox repeatedly to rotate through all three states.

**Permissions Summary**

| Permission Summary    | Grant New Permissions | Read Forum                          | Rate Message                        | Create Thread                       | Create Message                      | Create Attachment                   | Create Poll                         | Vote in Poll                        | Create Announce                     | Remove                              |
|-----------------------|-----------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| User Types            |                       |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |
| Anyone *              |                       | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Registered Users *    |                       | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Users                 |                       |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |
| monica                |                       | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |
| Groups                |                       |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |
| No group permissions. |                       |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |

11. In WebCenter Space, navigate to the group space's Discussions Forum Settings tab, to reassociate the group space with the discussion data that you just imported:
  - a. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator."](#)
  - b. Click the **Administration** link at the top of the application.
  - c. Click the **Group Spaces** tab.
  - d. From the **Actions** menu, choose **Edit Group Space**, for the group space you want to export.
  - e. Click the **Services** tab, then **Discussions**.
  - f. Click the **Search** icon besides Category ID or Forum ID, and choose the imported category (or forum) from the list.
  - g. Click **Apply**.

### 16.1.7.3 Exporting Wikis and Blogs for a Group Space

Use Oracle Data Pump utilities and the group space export script (`owc_wiki_export.sql`) to export wikis and blogs associated with a particular group space.

**See Also:** For more information, see "Oracle Data Pump" in *Oracle Database Utilities*.

During the export process, wikis and blogs stored on Oracle WebCenter Wiki schema are exported to the data pump directory (the `WC_PUMP_DIR` directory in the example below.)

Before you start, you must copy the group space export script provided with Oracle WebCenter (`WC_ORACLE_HOME/wikiserver/owc_wiki/WEB-INF/classes/owc_wiki_export.sql`) to the computer where you are running SQL. If you've already run the script, be sure to remove the dump file `WCWIKI_EXPDP.dmp` from the `WC_PUMP_DIR` directory before running the script again.

To export group space wikis and blogs:

1. Copy the group space export script from `/WC_ORACLE_HOME/wikiserver/owc_wiki/WEB-INF/classes/owc_wiki_export.sql` to the computer where you are running SQL, for example, `/myscripts/`.

2. Go to `ORACLE_HOME/bin` of your database where the Oracle WebCenter Wiki schema is installed, and connect to the database using `sqlplus` as the schema owner:

```
DB_OH/bin/sqlplus "<srcrcuprefix>_WIKI/password@dbhost"
```

3. Create the data pump directory (`data_pump_dir`):

```
SQL> create or replace directory WC_PUMP_DIR as '<full_path_to_a_directory_on_the_file_system>';
```

For example:

```
SQL> create or replace directory WC_PUMP_DIR as '/tmp/wikiData/';
```

4. Grant the Oracle WebCenter Wiki schema (`srcrcuprefix_WIKI`) read/write access to the data pump directory.

For example:

```
SQL> grant read, write on directory WC_PUMP_DIR to srcrcuprefix_WIKI;
```

5. Run `owc_wiki_export.sql`:

For example, if you copied the script to a directory called `/myscripts/`:

```
SQL> connect srcrcuprefix_
WIKI/password@//dbhost:dbport/service
```

```
SQL> @/myscripts/owc_wiki_export.sql
```

6. When prompted, enter the wiki domain associated with the group space.

`WCWIKI_EXPDP.dmp` is created in the `WC_PUMP_DIR`. For example, `/tmp/wikiData/`.

#### 16.1.7.4 Importing Wikis and Blogs for a Group Space

Use Oracle Data Pump utilities and the group space import script (`owc_wiki_import.sql`) to import group space wikis and blogs, exported from another WebCenter Spaces application.

**See Also:** For more information, see "Oracle Data Pump" in *Oracle Database Utilities*.

Before you start, you must copy the group space import script provided with Oracle WebCenter (`WC_ORACLE_HOME/wikiserver/owc_wiki/WEB-INF/classes/owc_wiki_import.sql`) to the computer where you are running SQL. If the source and target databases are different, you must edit this script, as described below.

The import script will import the data based on the domain name, so make sure the same domain name does not exist in the target schema before running the script. Also ensure that the associated group space exists on the target before you import the group space wikis and blogs. See [Section 16.1.8.1, "Exporting Group Spaces Using WebCenter Spaces"](#).

To import group space wikis and blogs:

1. Copy the group space import script from `WC_ORACLE_HOME/wikiserver/owc_wiki/WEB-INF/classes/owc_wiki_import.sql` to the computer where you are running SQL, for example, `/myscripts/`.
2. Copy the exported file, for example `WCWIKI_EXPDP.dmp`, to an appropriate directory on the target system.

For example:

```
SQL> cp /testserver/tmp/wikiData/WCWIKI_EXPDP.dmp
/productionserver/tmp/wikiDataTarget/WCWIKI_EXPDP.dmp
```

3. Go to `ORACLE_HOME/bin` of your database where Oracle WebCenter Wiki schema is installed, and connect to the database using `sqlplus` as the schema owner:

```
DB_OH/bin/sqlplus "<tgtrcuprefix>_WIKI/password@dbhost"
```

4. Grant the Oracle WebCenter Wiki schema (`tgtrcuprefix_WIKI`) read/write access to the data pump directory.

For example:

```
SQL> grant read, write on directory WC_PUMP_DIR to tgtrcuprefix_WIKI;
```

5. Create the `data_pump_dir`:

```
SQL> create or replace directory WC_PUMP_DIR as '<full_path_to_a_directory_on_the_file_system>';
```

For example:

```
SQL> create or replace directory WC_PUMP_DIR as
'/tmp/wikiDataTarget/';
```

6. If the source and target databases are different, edit the import script `/myscripts/owc_wiki_import.sql` as follows:

```
DBMS_DATAPUMP.METADATA_REMAP(dp_handle, 'REMAP_
SCHEMA', 'SOURCE_WIKI_SCHEMA', 'TARGET_WIKI_SCHEMA');
```

- a. **SOURCE\_WIKI\_SCHEMA** - replace with the source schema where you ran `owc_wiki_export.sql`
- b. **TARGET\_WIKI\_SCHEMA** - replace with the target schema where you will run `owc_wiki_import.sql`

7. Run `owc_wiki_import.sql`:

For example, if you copied the script to a directory called `/myscripts/`:

```
SQL> @/myscripts/owc_wiki_import.sql
```

### 16.1.7.5 Exporting Documents for a Group Space

After importing a group space you can use WebDAV to upload group space documents stored in Oracle Content Server to the new target; there is no need to export the content first.

### 16.1.7.6 Importing Documents for a Group Space

Before migrating group space documents to a new target you must enable the Documents service in the imported group space. Once the service is enabled, you can use WebDAV to upload group space documents onto the target system.

When dragging and dropping content to the target system, **do not** drag the group space folder to the target; you must only drag and drop content that is stored under the group space folder.

WebDAV is enabled on Oracle Content Server out-of-the-box. If you do not know the WebDAV URL for the Oracle Content Server that is used to store group space and personal space documents, contact your Fusion Middleware Administrator. If the base URL for that Oracle Content Server is `http://<host>:<port>/<relative_web_root>`, the WebDAV root URL will be `http://<host>:<port>/<relative_web_root>/idcplg/webdav`.

---

---

**Note:** Depending on the WebDAV client you use, all properties may not be copied over (for example, document descriptions, checkin and checkout status, and versions may not be carried across).

---

---

To set up the target group space and import documents from another group space:

1. In WebCenter Spaces, enable the Documents service in the imported group space:
  - a. Login to the WebCenter Spaces application that contains the imported group space.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator."](#)
  - b. Click the **Administration** link at the top of the application.
  - c. Click the **Group Spaces** tab.
  - d. From the **Actions** menu, choose **Edit Group Space**, for the imported group space.
  - e. Click the **Services** tab.
  - f. Select the check box next to **Documents** to enable this service, and then click **Apply**.
  - g. Click **OK** to dismiss the warning about permission configuration requirements.
  - h. Click the **Roles** tab, and assign appropriate **Documents** permissions to each group space role.
  - i. Click **Apply** to save.
2. Using WebDAV (for Oracle Content Server), drag and drop content from the folder belonging to the source group space to the empty folder assigned to the target group space.

### 16.1.8 Exporting Group Spaces

Administrators can export one or more group spaces using WebCenter Spaces and WLST commands.

Group space information is exported into a single export archive (.ear file). The EAR file contains a metadata archive (.mar file) and a single XML file containing the security policy information. You can save export group space archives to your local file system or to a remote server file system.

For more information about what is exported, see [Section 16.1.1, "Understanding WebCenter Spaces Export and Import"](#).

The export process does not include data associated with external group space services, such as, Discussions, Announcements, Wiki, Blogs, and Documents. To learn how to move data associated with these services, see [Section 16.1.7, "Migrating Back-end Components for Individual Group Spaces"](#).

---

---

**Note:** No icons, skins, images, or personalizations are exported. For information on personalizations, see the section "Personalizing Your Page View" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

---

---

This section includes the following:

- [Exporting Group Spaces Using WebCenter Spaces](#)
- [Exporting Group Spaces Using WLST](#)

If you want to export an entire WebCenter Spaces application, see [Section 16.1.4, "Exporting an Entire WebCenter Spaces Application"](#).

#### 16.1.8.1 Exporting Group Spaces Using WebCenter Spaces

WebCenter Spaces administrators can export one or more group spaces from WebCenter Spaces administration pages. For details, see [Section 23.1, "Exporting Group Spaces"](#).

#### 16.1.8.2 Exporting Group Spaces Using WLST

Use the WLST command `exportGroupSpaces` to export one or more group spaces. For command syntax and examples, see "exportGroupSpaces" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands"](#).

### 16.1.9 Importing Group Spaces

Administrators can import a group space archive (.EAR) using WebCenter Spaces and WLST commands.

On import, *all* group spaces included in the archive are created or re-created on the target application. Existing group spaces are deleted then replaced, and new group spaces are created.

All group spaces must have a security policy. When you import a brand new group space you must ensure that the group space's security policy is included in the export archive. Existing group spaces already have a security policy in place so, in this case, it's up to you whether to overwrite the security information on import or maintain the existing security policy.

If data migration is important, group space documents, discussions, and wikis and blogs can be migrated for individual group spaces. For details, see [Section 16.1.7, "Migrating Back-end Components for Individual Group Spaces"](#).

WebCenter Spaces does not support concurrent import operations. To avoid potential conflicts, import operations are disallowed while an import is in progress.

This section includes the following:

- [Importing Group Spaces Using WebCenter Spaces](#)

- [Importing Group Spaces Using WLST](#)

### 16.1.9.1 Importing Group Spaces Using WebCenter Spaces

WebCenter Spaces administrators can import a group space archive (.EAR) into another WebCenter Spaces application. For details, see [Section 23.2, "Importing Group Spaces"](#).

### 16.1.9.2 Importing Group Spaces Using WLST

Use the WLST command `importGroupSpaces` to import one or more group spaces. For command syntax and examples, see "importGroupSpaces" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands"](#).

## 16.1.10 Migrating Back-end Components for Group Space Templates

Group space templates do not contain any data; there is no need to migrate any back-end component data when you export and import group space templates.

## 16.1.11 Exporting Group Space Templates

Administrators can export group space templates and import them into other WebCenter Spaces applications. Out-of-the-box templates, such as the Group Project and Community of Interest templates, cannot be exported.

While export and import utilities are primarily used to move information between WebCenter Spaces applications, the group space template export feature is also useful as a backup service, and for sharing and exchanging templates with others.

Group space template information is exported into a single export archive (.EAR file). The EAR file contains a metadata archive (.MAR file) and a single XML file containing group space security policy information.

Group space templates include pages, metadata, roles, and service information only; no data, such as documents, discussion threads, and list data, is stored with the template.

You can save export archives to your local file system or to a remote server file system.

This section includes the following:

- [Exporting Group Space Templates Using WebCenter Spaces](#)
- [Exporting Group Space Templates Using WLST](#)

See also, [Section 16.1.8, "Exporting Group Spaces"](#).

### 16.1.11.1 Exporting Group Space Templates Using WebCenter Spaces

WebCenter Spaces administrators can export one or more group space templates from WebCenter Spaces administration pages. For details, see [Section 23.3, "Exporting Group Space Templates"](#).

### 16.1.11.2 Exporting Group Space Templates Using WLST

Use the WLST command `exportGroupSpaceTemplates` to export one or more group space templates. For command syntax and examples, see "exportGroupSpaceTemplates" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands"](#).

## 16.1.12 Importing Group Space Templates

Administrators can import a group space template archive (.EAR) into another WebCenter Spaces application.

On import, *all* group space templates included in the archive are re-created on the target application. If a group space template exists on the target, then it is deleted and replaced. If a group space template does not exist, then it is created.

Newly imported group space templates will be in a published/unpublished state depending upon the template's state when it was exported from the source. To find out how to change a template's state, see [Section 22.6, "Publishing and Unpublishing Group Space Templates"](#).

WebCenter Spaces does not support concurrent import operations. To avoid potential conflicts, import operations are disallowed while an import is in progress.

This section includes the following:

- [Importing Group Space Templates Using WebCenter Spaces](#)
- [Importing Group Space Templates Using WLST](#)

See also, [Section 16.1.9, "Importing Group Spaces"](#).

### 16.1.12.1 Importing Group Space Templates Using WebCenter Spaces

WebCenter Spaces administrators can import one or more group space templates from WebCenter Spaces administration pages. For details, see [Section 23.4, "Importing Group Space Templates"](#)

### 16.1.12.2 Importing Group Space Templates Using WLST

Use the WLST command `importGroupSpaces` to import one or more group space templates. For command syntax and examples, see "importGroupSpaces" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands"](#).

## 16.2 Exporting and Importing Custom WebCenter Applications for Data Migration

This section describes how to export and import metadata and customizations of a custom WebCenter application developed with Oracle WebCenter Framework.

It includes the following sections:

- [Understanding Custom WebCenter Application Export and Import](#)
- [Prerequisites for Custom WebCenter Application Export and Import](#)
- [Exporting Portlet Client Metadata \(Custom WebCenter Applications\)](#)
- [Importing Portlet Client Metadata \(Custom WebCenter Applications\)](#)
- [Exporting WebCenter Web 2.0 Services Metadata and Data \(Custom WebCenter Applications\)](#)



- [Importing WebCenter Web 2.0 Services Metadata and Data \(Custom WebCenter Applications\)](#)
- [Migrating Security for Custom WebCenter Applications](#)
- [Migrating Data \(Custom WebCenter Applications\)](#)

### 16.2.1 Understanding Custom WebCenter Application Export and Import

Several migration tools are available to export and import custom WebCenter applications, their connections and customizations (that is, customizations applied to an application, pages, and portlets) between stage and production environments (Figure 16–10).

**Figure 16–10 WebCenter Application Export and Import**

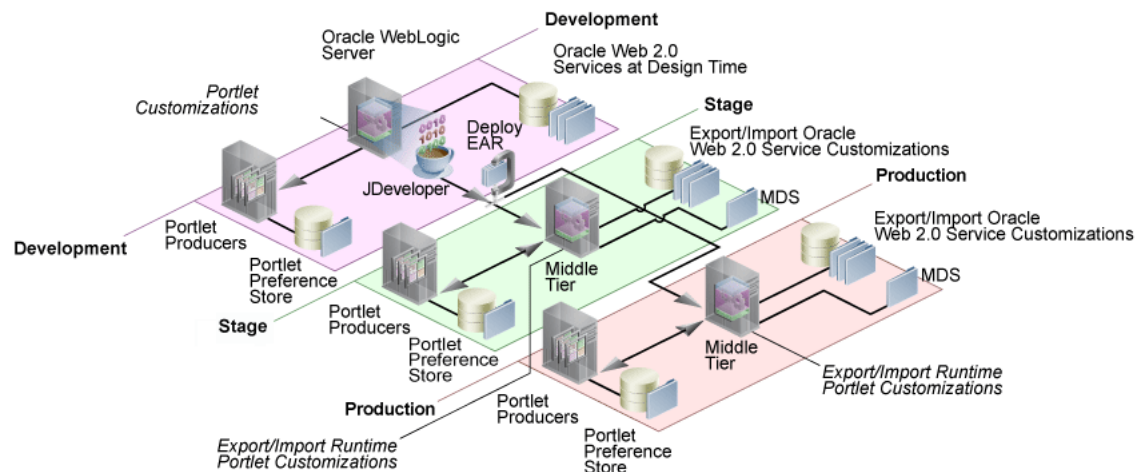


Table 16–4 lists available migration tools and their capabilities. All customizations listed in Table 16–1 are migrated with custom WebCenter applications.

**Table 16–4 Custom WebCenter Application Migration Tools**

| Migration Tools              | Capabilities   |
|------------------------------|--|
| Portlet Client WLST Commands | Enable export and import of portlet client metadata, and producer customizations and personalizations.   |
| MDS WLST Commands            | Enables export and import of: <ul style="list-style-type: none"> <li>■ WebCenter application metadata including customizations made to pages and Oracle WebCenter Web 2.0 Services</li> <li>■ Data stored in the <code>connections.xml</code> and <code>adf-config.xml</code> documents</li> </ul> |
| Migration WLST Commands      | Enables export and import of security policies, including roles and mapping of users and roles.  |
| Oracle Database Utilities    | Enables export and import of WebCenter application data. For information, see the part "Oracle Data Pump" in <i>Oracle Database Utilities</i> .  |

### 16.2.2 Prerequisites for Custom WebCenter Application Export and Import

The Oracle Database in which the application metadata and schema is stored must be up and running for the successful completion of the export and import operation.



The configured services in the target instance (the instance that is being imported into) must be a superset of what was configured in the instance that was exported. That is, the target must be configured with at least the same set of services that the source is configured with. If this is not the case, the import will fail.

### 16.2.3 Exporting Portlet Client Metadata (Custom WebCenter Applications)

To export portlet client metadata and producer customizations and personalizations, for a custom WebCenter application, use the WLST command `exportProducerMetadata`. This command is run on the entire application, and therefore, it exports metadata of all the producers stored in an application. You cannot opt to export metadata for specific producers.

For detailed syntax and examples, see "exportProducerMetadata" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands"](#)

For information on how to import portlet client metadata associated with all applications, see "Portlet Preference Store Migration Utilities" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

### 16.2.4 Importing Portlet Client Metadata (Custom WebCenter Applications)

This section describes how to import portlet client metadata and producer customizations and personalizations, for a custom WebCenter application, using the WLST command `importProducerMetadata`.

**Prerequisites:** The Oracle Database in which the application metadata or schema is stored and the portlet producers must be up and running.

To import portlet client metadata:

1. Start the WebLogic Scripting Tool (WLST) located at `WC_ORACLE_HOME/common/bin`.

On UNIX, start WLST using `wlst.sh`.

On Windows, use `wlst.cmd`.

See also, [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands"](#).

2. Run the WLST command `deleteMetadata` to delete the metadata under `/oracle/adf/portlet`.

```
deleteMetadata(application='application', server='server', docs='docs')
```

where:

- `application`: Name of the WebCenter application (for example, `sampleApp`)
- `server`: Name of the managed server (for example, `portletConsumer`).
- `docs`: List of comma separated fully qualified document name(s) and/or document name patterns (\* and \*\* patterns).

For example:

```
deleteMetadata(application='sampleApp', server='WLS_CustomApp',
docs='/oracle/adf/portlet/**')
```

For detailed syntax and examples, see "deleteMetadata" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

3. Run the WLST command `importProducerMetadata`:

```
importProducerMetadata(appName, fileName, server, applicationVersion)
```

where:

- `appName`: Name of the WebCenter application (for example, `sampleApp`).
- `fileName`: Name of the exported EAR file containing the portlet client metadata (for example, `export.ear`).
- `server`: Name of the managed server (for example, `portletConsumer`).
- `applicationVersion`: Version number of the deployed application, if more than one version of the application is deployed.

For detailed syntax and examples, see "importProducerMetadata" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*. See also the chapter "Metadata Services (MDS) Custom WLST Commands" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

## 16.2.5 Exporting WebCenter Web 2.0 Services Metadata and Data (Custom WebCenter Applications)

The metadata created by WebCenter Web 2.0 Services is stored in the Oracle metadata store (MDS). This section describes the transfer of the base documents and their customizations using WLST. For detailed information about MDS, see the chapter "Managing the Oracle Metadata Repository" in *Oracle Fusion Middleware Administrator's Guide*.

Customizations listed in [Table 16–1](#) are also exported when WebCenter applications are migrated between stage and production environments.

1. Start the WebLogic Scripting Tool (WLST) located at `WC_ORACLE_HOME/common/bin`.

On UNIX, start WLST is called `wlst.sh`.

On Windows, use `wlst.cmd`.

See also, [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands"](#).

2. Run the WLST command `exportMetadata`:

```
exportMetadata(application, server, toLocation, docs, [restrictCustTo],
[excludeAllCust], [excludeBaseDocs], [excludeExtendedMetadata], [fromLabel],
[toLabel], [applicationVersion])
```

For example:

```
exportMetadata(application='sampleApp', server='WLS_CustomApp',
toLocation='/tmp/myrepos', docs='/**')
```

For detailed syntax and examples, see "exportMetadata" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

---



---

**Note:** The `"/**"` command transfers all the documents required for all the services whose metadata is stored in the MDS repository. The structure of the stored content is `/application name/service name/...`

---



---

Where:

- `application`: Application name for which the metadata is to be exported (for example, `sampleApp`).
- `server`: Target server on which this application is deployed (for example, `WLS_CustomApp`).
- `toLocation`: Target directory to which documents selected from the source partition are to be transferred. The `toLocation` parameter can be used as a temporary file system for transferring metadata from one server to another.
- `docs`: List of comma separated fully qualified document name(s) and/or document name patterns (`*` and `**` patterns).
- `restrictCustTo`: List of customization layer names. This list is used to restrict the export of customization documents that match the specified customization layers. This option is ignored if the `excludeAllCust` option is also specified.
- `excludeAllCust`: Specifies whether to export all customization documents. This option overrides the `restrictCustTo` option.
- `excludeBaseDocs`: Specifies whether to export base documents.
- `excludeExtendedMetadata`: Specifies whether to export the Extended Metadata documents.
- `fromLabel`: If specified, transfers the documents from the source partition that is associated with this label.
- `toLabel`: If specified, works with the `fromLabel` variable to transfers the delta between `fromLabel` to `toLabel` from the source partition.
- `applicationVersion`: Application version in case multiple versions of the same application are deployed.

The metadata for WebCenter Web 2.0 Services, which consists of base and customization documents, are stored in the following paths:

- **Announcements:** `/oracle/webcenter/collab/announcement/**`
- **Documents:** `/oracle/webcenter/doclib/**` and `/oracle/webcenter/doclib/view/jsf/fragments/**`
- **Discussions:** `/oracle/webcenter/collab/forum/**`
- **General Settings:** `/oracle/webcenter/generalsettings/**`
- **Group Space**  
**Events:** `/oracle/webcenter/collab/calendar/community/**`
- **Lists:** `/oracle/webcenter/list/**` and `/oracle/webcenter/list/view/jsf/regions/**`
- **Mail:** `/oracle/webcenter/collab/mail/**`
- **Notes:** `/oracle/webcenter/note/**`
- **Page:** `/oracle/webcenter/page/**` and `/pageDefs/**`

- **Portlet:**
  - For each scope in the application:  
    `/oracle/adf/portlet/scopedMD/<scope GUID>/portlet.xml`
  - Producer MDS data and remote customizations export set
- **Recent Activity:** `/oracle/webcenter/recentactivity/**`
- **RSS News Feed:** `oracle/webcenter/rss/**`
- **Links:** `/oracle/webcenter/relationship/**`
- **Scope:** `/oracle/webcenter/framework/scope/**`
- **Search:** `/oracle/webcenter/search/**`
- **Tags:** `/oracle/webcenter/tagging/**`
- **adf-config.xml, connections.xml:**  
`/META-INF/mdssys/cust/adfshare/adfshare/**`

## 16.2.6 Importing WebCenter Web 2.0 Services Metadata and Data (Custom WebCenter Applications)

To import custom WebCenter application metadata and customizations:

1. Start the WebLogic Scripting Tool (WLST) located at `WC_ORACLE_HOME/common/bin`.

On UNIX, start WLST using `wlst.sh`.

On Windows, use `wlst.cmd`.

See also, [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands"](#).

2. Run the WLST command `importMetadata`:

```
importMetadata( application, server, fromLocation, docs, [restrictCustTo],  
[excludeAllCust], [excludeBaseDocs], [excludeExtendedMetadata],  
[cancelOnException], [applicationVersion])
```

For example:

```
importMetadata(application='sampleApp', server='WLS_CustomApp',  
fromLocation='/tmp/myrepos', docs='/**')
```

Where:

- `application`: Application name for which the metadata is be imported (for example, `sampleApp`).
- `server`: Name of the target server on which this application is deployed (for example, `WLS_CustomApp`).
- `fromLocation`: Source directory from where documents are selected for the transfer. The `fromLocation` parameter can be used as a temporary file system location for transferring metadata from one server to another.
- `docs`: List of comma separated fully qualified document name(s) and/or document name patterns (\* and \*\* patterns).
- `restrictCustTo`: List of customization layer names. This list is used to restrict the import of customization documents that match the specified

customization layers. This option is ignored if the `excludeAllCust` option is also specified.

- `excludeAllCust`: Specifies whether to import all customization documents. This option overrides the `restrictCustTo` option.
- `excludeBaseDocs`: Specifies whether to import base documents.
- `excludeExtendedMetadata`: Specifies whether to import the Extended Metadata documents.
- `cancelOnException`: Whether to terminate the import operation when an exception is encountered. On termination, the delete is rolled back if supported by the target store.
- `applicationVersion`: Application version in case multiple versions of the same application are deployed.

For detailed syntax and examples, see "importMetadata" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

## 16.2.7 Migrating Security for Custom WebCenter Applications

Security migration involves moving the identity store, credential store, and policy store, from one WebCenter application to another. The process is the same for all WebCenter applications so, for custom WebCenter applications, you can follow the same instructions provided for WebCenter Spaces:

- [Exporting the LDAP Identity Store](#)
- [Importing the LDAP Identity Store](#)
- [Exporting and Importing the LDAP Credential Store](#)
- [Exporting and Importing the LDAP Policy Store](#)

## 16.2.8 Migrating Data (Custom WebCenter Applications)

To export the custom WebCenter application data, use the export and import database utilities. This section includes the following sub sections:

- [Exporting Data \(Custom WebCenter Applications\)](#)
- [Importing Data \(Custom WebCenter Applications\)](#)

### 16.2.8.1 Exporting Data (Custom WebCenter Applications)

To export the custom WebCenter application data, use the Oracle Data Pump export utility. For example, go to `ORACLE_HOME/bin` of your database and run the command described in [Example 16–11](#).

**See Also:** For more information, see "Oracle Data Pump" in *Oracle Database Utilities*.

#### **Example 16–11 Data Pump Utility (Export)**

```
DB_OH/bin/expdp \"sys/password@dbhost as sysdba\" SCHEMAS=rcuprefix_WEBCENTER
DIRECTORY=data_pump_dir DUMPFILE=wc.dmp
```

where:

- `DB_OH` is the directory in which the database for the Oracle WebCenter schema is installed.

- password is the password for system database user.
- dbhost is the host name of the database.
- SCHEMAS is the schema of the database. This is the RCU suffix that was used during installation along with the suffix \_WEBCENTER. For example, DEV\_WEBCENTER.
- DIRECTORY specifies the directory object created for the export and import operation.

---

**Note:** The data\_pump\_dir file must have been created in SQL using a tool like SQL\*Plus. For example:

```
SQL> create or replace directory DATA_PUMP_DIR as '<full_path_to_a_directory_on_the_file_system>';
SQL> commit;
SQL> quit
```

---

- DUMPFILE contains the exported data. This file is used during import.

### 16.2.8.2 Importing Data (Custom WebCenter Applications)

To import data for custom WebCenter applications, use the Oracle Data Pump import utility. For example, go to `ORACLE_HOME/bin` of your database and run the command described in [Example 16–12](#).

**See Also:** For more information, see "Oracle Data Pump" in *Oracle Database Utilities*.

#### **Example 16–12 Data Pump Utility (Import)**

```
DB_OH/bin/impdp \"sys/password@dbhost as sysdba\" REMAP_SCHEMA=srcrcuprefix_
WEBCENTER:prdrucuprefix_WEBCENTER
DIRECTORY=data_pump_dir DUMPFILE=wc.dmp TABLE_EXISTS_ACTION=REPLACE
```

where:

- DB\_OH is the directory in which the database for the Oracle WebCenter schema is installed.
- password is the password for system database user.
- dbhost is the host name of the database.
- REMAP\_SCHEMA maps the schema exported from the stage environment to the schema in the production environment. This is the RCU suffix that was used during installation along with the suffix \_WEBCENTER. For example, DEV\_WEBCENTER.
- DIRECTORY specifies the directory object created for the export and import operation.

---

---

**Note:** The `data_pump_dir` file must have been created in SQL using a tool like SQL\*Plus. For example:

```
SQL> create or replace directory DATA_PUMP_DIR as '<full_path_to_a_directory_on_the_file_system>';
SQL> commit;
SQL> quit
```

---

---

- `DUMPFILE` contains the data to be imported.
- `TABLE_EXISTS_ACTION` replaces the existing table with the imported table.

## 16.3 Backing Up and Recovering WebCenter Applications

To recover data from disasters, such as the loss of database hardware, inadvertent removal of data from file or database, it is important to back up WebCenter applications on a frequent basis. The frequency of backup depends on how often the underlying information stored by WebCenter changes in a particular customer application, and how much time and amount of information could acceptably be lost. Incremental or partial backups may be applied where the data is critical to the business and must be restored due to a failure.

Backup and recovery of WebCenter components can be managed through database export and import utilities, and various other tools. For more information, see "Part IV Advanced Administration: Backup and Recovery" in *Oracle Fusion Middleware Administrator's Guide*.





# Part V

---

## Application Administration for Oracle WebCenter Spaces

Part IV contains the following chapters:

- [Chapter 17, "Accessing WebCenter Spaces Administration Pages"](#)
- [Chapter 18, "Customizing WebCenter Spaces"](#)
- [Chapter 19, "Managing Users and Roles for WebCenter Spaces"](#)
- [Chapter 20, "Managing Pages in WebCenter Spaces"](#)
- [Chapter 21, "Making Applications Available in WebCenter Spaces"](#)
- [Chapter 22, "Managing Group Spaces in WebCenter Spaces"](#)
- [Chapter 23, "Exporting and Importing Group Spaces"](#)



## Accessing WebCenter Spaces Administration Pages

This chapter describes how to access administration pages in the WebCenter Spaces application. It contains the following subsections:

- [Logging into WebCenter Spaces as an Administrator](#)
- [WebCenter Spaces Administration Pages](#)

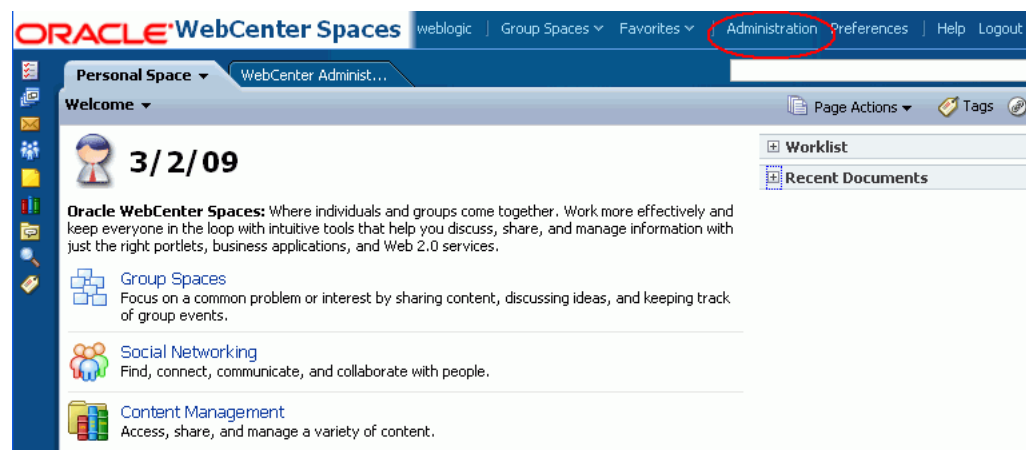
### Audience

The content of this chapter is intended for WebCenter Spaces administrators. Users granted the WebCenter Spaces Administrator role or a custom role that grants the Application-Manage permission).

## 17.1 Logging into WebCenter Spaces as an Administrator

WebCenter users with administrative privileges will see an **Administration** link at the top of the application when they log in ([Figure 17-1](#)).

**Figure 17-1 Administration Link**



The **Administration** link provides access to administration and application settings for WebCenter Spaces. For more detail, see [Section 17.2, "WebCenter Spaces Administration Pages"](#).

---



---

**Note:** If you do not see this link, you do not have administrative privileges. Ask your WebCenter Spaces Administrator to check the permissions assigned to your role.

---



---

WebCenter Spaces administrators may assign administrative privileges to other users, if required. For more information, see [Section 19.2.4, "Giving a User Administrative Privileges"](#).

To log in to WebCenter Spaces.

1. Open WebCenter Spaces using the following URL:

`http://<host>:<port>/webcenter`

If you do not know which host or port to use, ask your systems administrator. See also, "Managing Ports" in *Oracle Fusion Middleware Administrator's Guide*.

If you have access to Fusion Middleware Control, this information is available on the WebCenter Space home page. See [Section 6.2, "Navigating to the Home Page for WebCenter Spaces"](#).

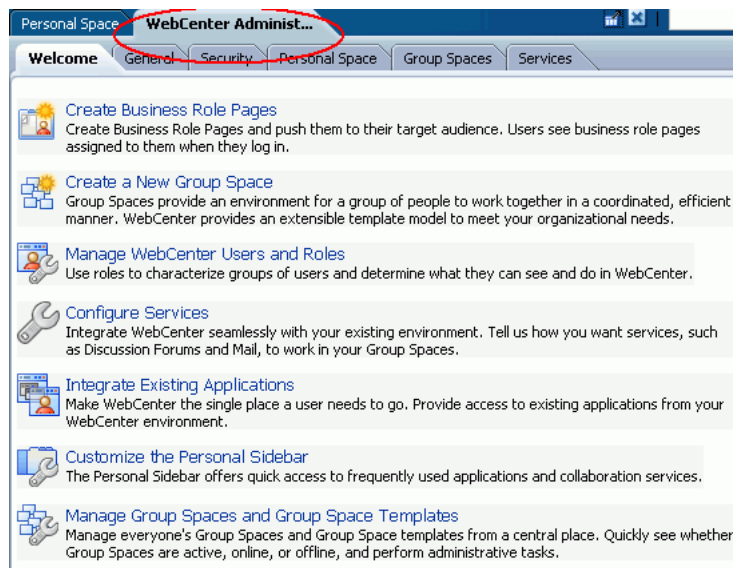
2. Enter your user name in the **User Name** field and your password in the **Password** field.
3. Click **Login**.

Check that you can see the **Administration** link at the top of the application ([Figure 17-1](#)).

## 17.2 WebCenter Spaces Administration Pages

There are six WebCenter Administration pages—Welcome, General, Security, Personal Space, Group Spaces, and Services ([Figure 17-2](#)):

**Figure 17-2 WebCenter Administration Pages**



Administrators can perform all their administrative duties from here:

| Administration Page | Description  |
|---------------------|--|
| Welcome             | This page is a convenient launching pad for some common administrative tasks. Click a task link to navigate to the appropriate page.   |
| General             | <p>Use this page to customize WebCenter Spaces. For example, you can specify a default language, application name, and so on. For more information, see:</p> <ul style="list-style-type: none"> <li><a href="#">Chapter 18, Naming Your WebCenter</a></li> <li><a href="#">Chapter 18, Changing the WebCenter Logo</a></li> <li><a href="#">Chapter 18, Applying Look and Feel using Skins</a></li> <li><a href="#">Chapter 18, Choosing the Default Display Language</a></li> <li><a href="#">Chapter 18, Customizing Copyright and Privacy Statements</a></li> <li><a href="#">Chapter 18, Customizing the Online Help Link</a></li> <li><a href="#">Chapter 18, Enabling and Disabling Personal Spaces</a></li> <li><a href="#">Chapter 19, Allowing Self-Registration</a></li> <li><a href="#">Chapter 20, Customizing the Self-Registration Page</a></li> <li><a href="#">Chapter 20, Customizing the Login Page</a></li> </ul> |
| Security            | <p>Use this page to manage WebCenter users and roles. For more information, see:</p> <ul style="list-style-type: none"> <li><a href="#">Chapter 19, Managing Users and Roles for WebCenter Spaces</a></li> </ul>   |
| Personal Space      | <p>Use this page to manage pages for personal spaces and WebCenter Spaces, and to customize everyone's sidebar. For more information, see:</p> <ul style="list-style-type: none"> <li><a href="#">Chapter 20, "Managing Pages in WebCenter Spaces"</a></li> <li><a href="#">Chapter 18, Customizing the Sidebar</a></li> </ul>   |
| Group Spaces        | <p>Use this page to manage group spaces and group space templates. For more information, see:</p> <ul style="list-style-type: none"> <li><a href="#">Chapter 22, Managing Group Spaces in WebCenter Spaces</a></li> <li><a href="#">Chapter 22, Managing Group Space Templates</a></li> </ul>  |
| Services            | <p>Use this page to set application-wide properties for discussion forums and announcements and everyone's personal profiles. For more information, see:</p> <ul style="list-style-type: none"> <li><a href="#">Chapter 18, Setting Discussion Forum Options</a></li> <li><a href="#">Chapter 18, Managing Personal Profiles</a></li> </ul>  |



---

---

## Customizing WebCenter Spaces

This chapter describes how to customize WebCenter Spaces for your target audience. You must login to WebCenter Spaces with administrative privileges to set any of the application-wide properties described here.

This chapter includes the following sections:

- [Naming Your WebCenter](#)
- [Customizing the Online Help Link](#)
- [Customizing the Sidebar](#)
- [Changing the WebCenter Logo](#)
- [Applying Look and Feel using Skins](#)
- [Customizing Copyright and Privacy Statements](#)
- [Choosing the Default Display Language](#)
- [Setting Discussion Forum Options](#)
- [Managing Personal Profiles](#)
- [Enabling and Disabling WebCenter Services](#)
- [Enabling and Disabling Personal Spaces](#)
- [Publishing the WebDAV URL](#)
- [Overriding and Customizing Application Templates](#)
- [Making New Page Styles Available](#)
- [Customizing the Resource Catalog and Deploying New Task Flows](#)

### **Audience**

The content of this chapter is intended for WebCenter Spaces administrators. Users granted the WebCenter Spaces Administrator role or a custom role that grants the Application-Manage permission).

## 18.1 Naming Your WebCenter

Out-of-the-box, the application name *WebCenter Spaces* appears in the banner (see [Figure 18-1](#)). If you prefer, you can change the name to better suit your target audience. For example, you might want to display your company name here or the name of a department within your company.

**Figure 18–1 Naming Your WebCenter**



**Note:** You can change the logo that displays next to the application name too. See [Section 18.4, "Changing the WebCenter Logo"](#).

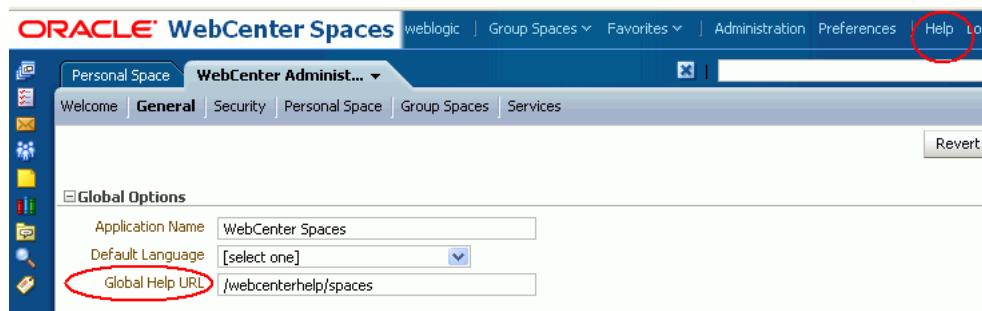
To change the name of your WebCenter Spaces application:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **General** tab.
4. In the **Application Name** field, enter the new name.  
Alphanumeric characters are allowed together with spaces, underscores (\_) and dashes (-). For example, Finance Department - My Corporation.
5. Click **Apply**.

## 18.2 Customizing the Online Help Link

Online help for WebCenter Spaces displays when you click the Help link located at the top of the application (see [Figure 18–2](#)). Out-of-the-box, this Help link opens Oracle's built-in help. If you want, you can write online help specifically aimed at your end-users and redirect the Help link to a different help location.

**Figure 18–2 Customizing the Help Link**



When you customize the Help link, built-in help for WebCenter Spaces is still available through help buttons, help icons, and so on.

To customize the main Help link for WebCenter Spaces:



1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **General** tab.
4. In the **Global Help URL** field, enter the location of your help ([Figure 18-2](#)).

Ensure that you enter a fully qualified URL. For example:  
`http://<myhost>:<port>/myhelp`

The default Global Help URL is `/webcenterhelp/spaces`. This URL opens Oracle Help for the Web (OHW) and displays Oracle's built-in help for WebCenter Spaces.

---

**Note:** If you leave the Global Help URL field blank, the Help link is not displayed.

---

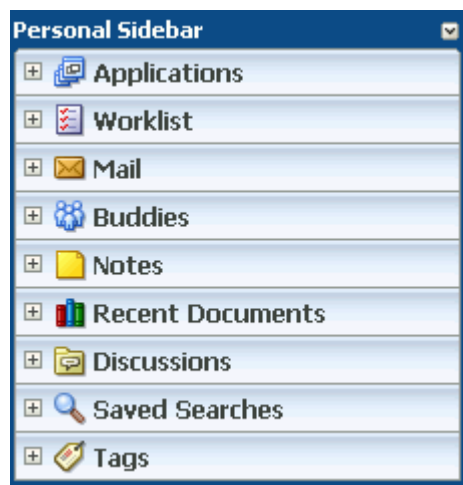
5. Click **Apply**.

Click **Help** at the top of the application to check the custom help opens correctly.

## 18.3 Customizing the Sidebar

The Sidebar in WebCenter Spaces offers users quick access to personal services such as mail, worklist assignments, personal contacts, and more. Out-of-the-box, the Sidebar will offer the full range of WebCenter services that are available and WebCenter users can hide any services they do not use or require.

**Figure 18-3** *The Sidebar*



The Sidebar is configurable. WebCenter Spaces administrators can customize the default sidebar for all users as follows:

- [Hiding and Showing Task Flows in the Sidebar](#)
- [Locking Sidebar Content](#)

### 18.3.1 Hiding and Showing Task Flows in the Sidebar

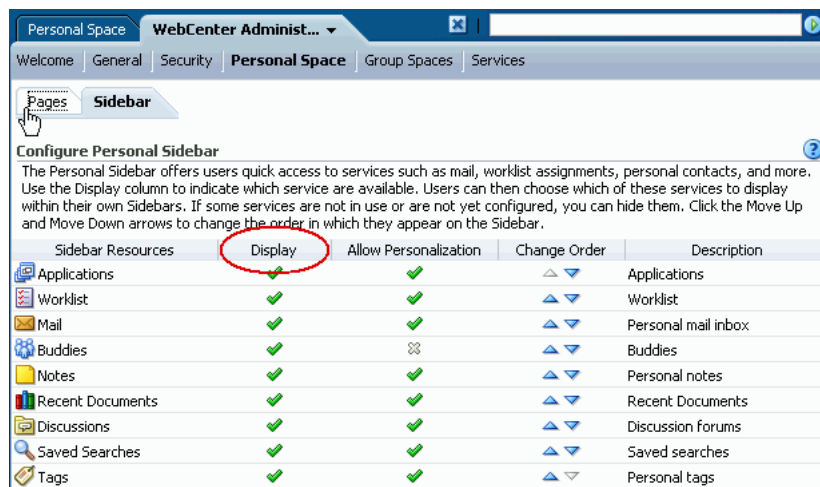
Administrators can choose which services are available through the sidebar and the order they are displayed. If some services are not in use or not yet configured you can hide them.

If you want to hide the entire sidebar, hide all available services.

To hide or show services on the sidebar:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Personal Space** tab.
4. Click the **Sidebar** tab.
5. Set the **Display** option ([Figure 18–4](#)):
  - Click the gray cross to show an item on the sidebar (cross changes to check mark).
  - Click the green check mark to hide an item on the sidebar (check mark changes to cross).

**Figure 18–4 Customizing the Sidebar**



6. Use the **Move Up** and **Move Down** arrows to change the display order.

Any changes you make immediately impact everyone's personal sidebar.

### 18.3.2 Locking Sidebar Content

Users can personalize their sidebar, that is, display sidebar panes when they require them and hide sidebar panes that they do not need or use. Sidebar personalization is useful for hiding non-essential services but might prove less desirable for sidebar content that is critical for user productivity. By locking individual panes on the sidebar, WebCenter Spaces administrators can control which resources always display and which resources never display.

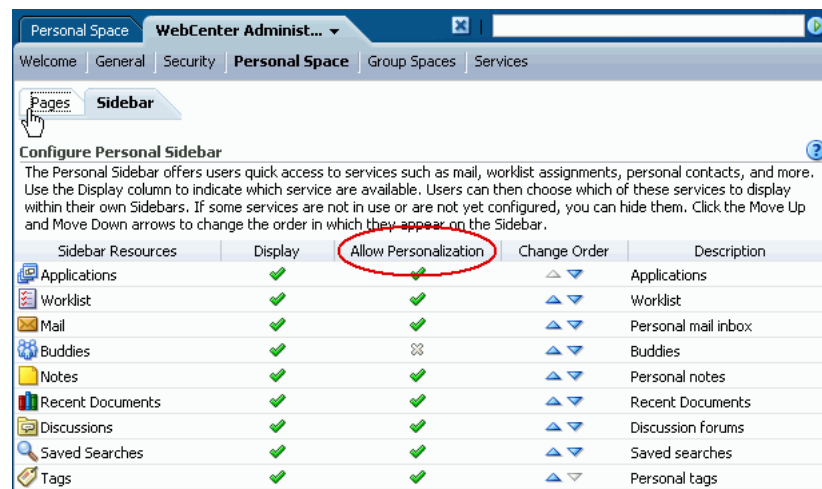
To lock sidebar content:

1. Login to WebCenter Spaces with administrative privileges.

See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).

2. Click the **Administration** link at the top of the application.
3. Click the **Personal Space** tab.
4. Click the **Sidebar** tab.
5. Set **Allow Personalization** ([Figure 18-5](#)):
  - Click the gray cross to allow user personalization (cross changes to check mark).
  - Click the green check mark to prevent user personalization (check mark changes to cross).

**Figure 18-5 Controlling Sidebar Personalization**



Any changes you make immediately impact everyone's personal sidebar.

## 18.4 Changing the WebCenter Logo

One way to apply corporate branding to WebCenter Spaces, is to add your company logo to the top left corner of the application ([Figure 18-6](#)). If your company's logo is not suitable, any graphic that brings visual interest can be used.

---

**Note:** You can change the application name that displays next to the logo too. See [Section 18.1, "Naming Your WebCenter"](#).

---

The logo you specify will resize automatically, according to the application skin.

**Figure 18–6 Changing the WebCenter Logo**

To change the WebCenter logo:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **General** tab.
4. Click **Browse** for the **Application Logo** property.  
The File Upload dialog box opens.
5. Select the logo you want to use.
6. Click **Apply** to save.

The logo is uploaded to the WebCenter Spaces image directory (`/webcenter/images`) and the new logo immediately appears in the top left corner of the application banner.

## 18.5 Applying Look and Feel using Skins

As WebCenter Spaces Administrator, you may customize the appearance of WebCenter Spaces for all users by changing its skin. A skin changes the way the user interface appears, but does not change the application's behavior. A selection of built-in skins are provided with WebCenter Spaces. Alternatively, create skins of your own and brand the application according to your corporate image.

### 18.5.1 What You Should Know About Application Skins

The look and feel of WebCenter Spaces is driven by an ADF Faces skin. A skin in ADF Faces is a global style sheet for the entire application. Every component in WebCenter Spaces will automatically use the styles described by this skin. ADF Faces skins are based on the Cascading Style Sheet specification, and use CSS 3.0 syntax.

Out-of-the-box, WebCenter Spaces uses the *Deep Sea* skin. In addition, WebCenter Spaces provides several built-in skins, with names such as *Storm* and *Midnight*, so that you can experiment with some different look and feels. For details, see [Section 18.5.2, "Selecting a Skin"](#).

If none of the built-in skins suit your requirements or you want to apply a look and feel that reflects your corporate brand, you may provide your own ADF Faces skin and apply it to WebCenter Spaces. For details, see [Section 18.5.3, "Making New Skins Available to WebCenter Spaces"](#).

## 18.5.2 Selecting a Skin

To apply a different skin to your WebCenter Spaces application:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **General** tab.
4. Choose an **Application Skin** from the list provided.

The skin list provided is generated from a file called `trinidad-skins.xml`. To add skins to this file, read [Section 18.5.3, "Making New Skins Available to WebCenter Spaces"](#).

5. Click **Apply**.

The selected skin is immediately applied to WebCenter Spaces.

## 18.5.3 Making New Skins Available to WebCenter Spaces

If none of the built-in skins suit your requirements or you want to apply a look and feel that reflects your corporate brand, you may provide your own ADF Faces skin and apply it to WebCenter Spaces.

Because newly deployed skins only become available to WebCenter Spaces once the application's managed server is restarted, custom skin deployment typically takes place before the WebCenter Spaces application goes live or during scheduled maintenance periods.

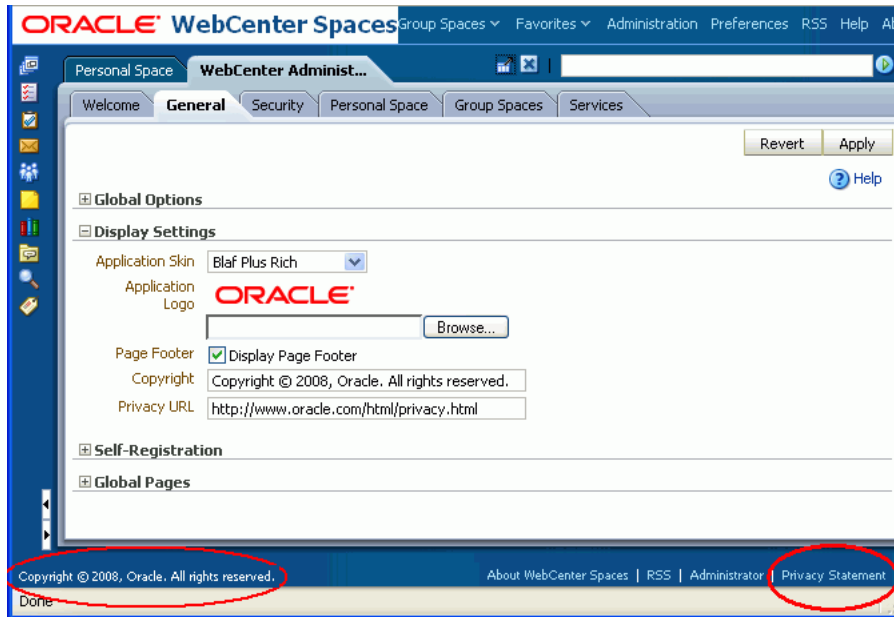
Custom skin deployment is described in a whitepaper entitled "*Extending WebCenter Spaces*" available on the Oracle Technology Network (<http://webcenter.oracle.com>).

## 18.6 Customizing Copyright and Privacy Statements

Administrators can customize or hide copyright and privacy statements for WebCenter Spaces. If displayed, the copyright and privacy URL appear in the application's page footer ([Figure 18-7](#)):

- Copyright - Displays a copyright statement for the entire application.
- Privacy URL - Links to a document that contains a privacy policy for the entire application.

**Figure 18–7 Customizing the Copyright and Privacy URL**



Individual group spaces may provide their own copyright and privacy statements. See "Customizing Copyright and Privacy Statements" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

To customize or hide copyright and privacy statements:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **General** tab.
4. Do one of the following:
  - Select **Display Page Footer** to display copyright and privacy information at the bottom of the application.
  - Deselect **Display Page Footer** to hide the page footer. No legal notices will display.
5. If you have chosen to display legal notices:
  - **Copyright** - Enter a suitable copyright statement for the WebCenter Spaces application. If no copyright information is required, leave this field blank.
  - **Privacy URL** - Specify the location of the application's privacy policy. Enter a fully qualified URL. If no privacy information is required, leave this field blank.
6. Click **Apply** to save.

New settings immediately display in the page footer.

## 18.7 Choosing the Default Display Language

The WebCenter Spaces application is translated into the following languages:

**Table 18–1 Languages Available for Oracle WebCenter Spaces**

| <b>A to Fi</b>        | <b>Fr to No</b> | <b>P to T</b> |
|-----------------------|-----------------|---------------|
| Arabic                | French          | Polish        |
| Brazilian Portuguese  | German          | Portuguese    |
| Chinese (Simplified)  | Greek           | Romanian      |
| Chinese (Traditional) | Hebrew          | Russian       |
| Czech                 | Hungarian       | Slovak        |
| Danish                | Italian         | Spanish       |
| Dutch                 | Japanese        | Swedish       |
| English               | Korean          | Thai          |
| Finnish               | Norwegian       | Turkish       |

Application content is translated, including links, field labels, display text, message text, and dialog boxes. However, information that users add to WebCenter Spaces such as announcements, documents, discussion forum content, and the like, is not translated. All user supplied content displays only in the language used by its author.

It is the administrator's job to choose a default *display language* for WebCenter Spaces. When picking the default language, consider which language suits the majority of people using the application. The first time a user logs in to WebCenter Space the default language displays but individuals can personalize their display language through user preferences.

The default display language only applies when users log in to WebCenter Spaces. All public pages, such as the welcome page and login page, display in the *browser language*.

WebCenter Spaces provides a language switcher on the welcome, login, and self registration pages to accommodate anyone whose native language is not the browser language. The language switcher sets the *session language cookie* which overrides the browser language and any default display language you may define for the application. The session language is retained for the life of the session cookie. When a user clears browser cookies—deliberately—the session language is also cleared and the browser language (unauthenticated) and default display language (authenticated) become active again.

To summarize, the order of precedence for WebCenter Spaces display language settings from weakest to strongest is as follows:

- **Browser language** - your Browser documentation will describe how to change the browser's language.
- **Application display language** - see instructions below.
- **User-defined display language** - see "Choosing Your Preferred Display Language" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.
- **Session language** - see "Setting a Session Display Language" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

To select the default display language for WebCenter Spaces:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).

2. Click the **Administration** link at the top of the application.
3. Click the **General** tab.
4. Choose a **Default Language**.
5. Click **Apply**.

The new language is effective immediately.

## 18.8 Setting Discussion Forum Options

Discussion forums allow group space members to capture, share, and preserve content that is relevant to their project or community goals.

As WebCenter Spaces Administrator, you are responsible for setting discussion forum options through WebCenter Spaces Administration (Figure 18–8).

**Figure 18–8** Setting Discussion Forum Options

The screenshot shows the 'WebCenter Administration' interface. The top navigation bar includes 'Welcome', 'General', 'Security', 'Personal Space', 'Group Spaces', and 'Services'. Below this is a 'Configure WebCenter Services' section with a 'Revert' and 'Apply' button. The main content area is titled 'Discussion Forum Settings' and is divided into three sections:

- General:**
  - Discussion Server: `http://stahx12.us.oracle.com:7005/owc_discussions`
  - Root Category: Specify the root category under which all WebCenter Spaces discussion forums are stored. Click the Find icon to select a category.
    - Category ID:  (with a search icon)
    - Category Name: WebCenter
- Default Group Space Forum:**
  - To create a default discussion forum for each new group space, select Create Default Forum, and then enter a suitable name and description for the default forum.
  - Create Default Forum
  - \* Forum Name:
  - Forum Description:
- Mail Settings:**
  - Mail communication through group space mail distribution lists can be published as discussion forum posts and archived on the discussions server. Use these options to identify the mail server and mail account used to receive group space mail.
  - Mail Account Details:
    - User name:
    - Password:
  - Mail Server Details:
    - IMAP Host:
    - IMAP Port:
    - Use SSL

From here, you can configure the following:

- [Specifying Where Discussions and Announcements are Stored on the Discussions Server](#)
- [Setting Up a Default Group Space Discussion Forum](#)
- [Enabling Discussion Forums to Publish Group Space Mail](#)



---



---

**Note:** The Fusion Middleware Administrator maintains the connection between WebCenter Spaces and the discussions server. If you are experiencing issues with this connection, report the problem to the Fusion Middleware Administrator. See also, [Section 11.1, "Setting Up Connections for the Discussions and Announcements Services"](#).

---



---

### 18.8.1 Specifying Where Discussions and Announcements are Stored on the Discussions Server

Administrators can change the root category (on the discussions server) under which all WebCenter Spaces discussions and announcements are stored.

If the root category is not defined within the connection, WebCenter is selected by default. You can choose a different location if you wish. This might be useful when WebCenter Spaces is connected to a discussions server that is hosting discussion forums for multiple applications.

Oracle recommendations:

- Choose a category that is dedicated to this WebCenter Spaces application. There may be conflicts when multiple WebCenter Spaces applications share the same root category.
- Do not switch the root category once WebCenter Spaces is up and running. If you change the root category, all the discussion forums under the old root will continue to work but you cannot, use the Links service to, create links to discussions or announcements stored in the old category.

Group spaces either own a category (supporting multiple forums) or a single forum, under the root category that you specify. It is the group space's template that determines whether it can support multiple forums. For example:

- **Communities of interest** - A sub category is created under the root category for each new group space based on the Community of Interest template.
- **Group projects** - As single forum is created under the root category for each new group space based on the Group Project template.
- **Group spaces based on blank templates** - By default, a single forum is created under the root category for each new group space based on the Blank template. Your systems administrator might override this if they feel that a sub category, that supports multiple forums, is more suitable. See also, [Section 11.1.3, "Registering Discussion Servers"](#).

To specify where WebCenter Spaces discussion forums are stored:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Services** tab, and then select **Discussions**.
4. Specify an appropriate **Root Category** for storing WebCenter Spaces discussions.  
Click the **Find** icon to view the categories available and then select the most appropriate location.

To create a new category especially for this WebCenter Spaces application, click **Create Category**. You must have system administrator permissions on the discussions server to create new categories.

5. Click **Apply** to save the settings.

## 18.8.2 Setting Up a Default Group Space Discussion Forum

Out-of-the box, a default discussion forum is provided for any group space that is based on the Community of Interest template and this default forum is named after the group space.

Group spaces that are based on the Community of Interest template support multiple forums. If you want, you can choose your own name and description for the default forum in these group spaces or you can disable the default forums feature altogether.

Default forum properties do not apply to group spaces based on the Group Project template. Project-based group spaces offer a single discussion forum that is always available and named after the group space.

To set up or disable the default discussion forum:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Services** tab, and then select **Discussions**.
4. Select **Create Default Forum** to always provide a default forum in group spaces based on Community of Interest templates.

Deselect this option to disable this feature. Group space moderators and members with the `Discussions-Manage` permission can create a discussion forum as and when one is needed.

5. If a default discussion forum is required:
  - a. Use **Forum Description** to specify a name for the default discussion forum.  
If you want to include the name of the parent group space in the forum name, include the syntax `#{groupSpace.description}`. For example: `General - #{groupSpace.description}`
  - b. Use the syntax `#{groupSpace.description}` in **Forum Description** to create a description based on the group space's name. For example:  
  
This is a general discussion forum for the `#{groupSpace.description}` group space.  
  
In this example, a group space named 'Photography', has a default discussion forum with the following description: This is a general discussion forum for the Photography group space.
6. Click **Apply** to save the settings.

## 18.8.3 Enabling Discussion Forums to Publish Group Space Mail

Mail communication through group space mail distribution lists can be published as discussion forum posts and archived on the discussions server. To enable this feature in WebCenter Spaces you must specify the mail server and mail account used to receive group space mail. WebCenter Spaces will monitor mail sent to this account and publish mail content on the appropriate group space discussion forum.

To ensure mail is not missed, the user account that you specify must be a member of every group space mail distribution list, that is, the user must be listed as a *default user* on the LDAP Directory Server. Default users are configured using a mail server connection property called **LDAP Default User**; this property takes multiple user names. See, [Section 11.3, "Setting Up Connections for the Mail Service"](#).

Once you have set up the mail server and mail account used to receive group space mail for all of WebCenter Spaces, it's up to the moderator of each group space to say which mail distribution list is monitored and which discussion forum is used to publish the group space mail. While it is possible for multiple group spaces to use the same distribution list it is archived only once. See also "Publishing Group Space Mail in a Discussion Forum" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

To configure the mail server used to receive and store group space mail:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Services** tab, and then select **Discussions**.
4. Configure **Mail Settings**:
  - a. Enter the **User Name** and **Password** for the mail account used to receive group space mail.  
The user specified here must be listed as a default user on the LDAP Directory Server. See, [Section 11.3, "Setting Up Connections for the Mail Service"](#).
  - b. Enter the **Host** name and **Port** of the IMAP mail server used to receive group space mail.  
Specify the mail server that is managing all group space distribution lists.
  - c. Enable or disable secure (encrypted) communication between WebCenter Spaces and the mail server.  
If you enable this option, the mail server must support SSL.
5. Click **Apply** to save the settings.

## 18.9 Managing Personal Profiles

Every WebCenter user has a personal profile that displays personal information such as their email address, phone number, office location, department, manager, direct reports, and so on. Most profile data originates from the back-end identity store that WebCenter Spaces is using ([Figure 18-9](#)).

**Figure 18–9 Personal Profile**



Personal profiles are presented in four sections: **Summary**, **Employee**, **Business Contact**, **Personal Information**. Each section provides information related to the section heading. For example, **Summary** includes a collection of basic details, such as the user's name, mail address, and office location.

It's the administrator's job to specify what information displays in each section, and whether users are allowed to edit their profile data and their password within WebCenter Spaces.

To manage personal profiles for WebCenter Spaces:

1. Log in to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Services** tab, and then select **Profiles** (Figure 18–10)

**Figure 18–10 Profile Management Settings**

**Profile Management Settings**

**Profile Access**  
Specify whether users can change their WebCenter password in WebCenter Spaces  
Allow password change

**Profile Access**  
Personal profiles present user information in the sections listed here. Use these settings to control which profile sections display and whether users are allowed to update their profile details

| Profile Section      | Available                           | Can Edit                            |
|----------------------|-------------------------------------|-------------------------------------|
| Summary              | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |
| Employee             | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Business Contact     | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |
| Personal Information | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |

**Profile Attributes**  
Each profile section displays several user attributes. If section updates are allowed, use these settings to specify exactly which profile attributes WebCenter users may update and those that are read-only

| Profile Section | Attribute    | Allow Update             |
|-----------------|--------------|--------------------------|
| Summary         | Email        | <input type="checkbox"/> |
|                 | Organization | <input type="checkbox"/> |
|                 | Title        | <input type="checkbox"/> |
|                 | Time Zone    | <input type="checkbox"/> |

4. Select **Allow Password Change** to allow WebCenter users to change their WebCenter Space login password through user preferences.

Clear this check box to prevent users from changing their login passwords through WebCenter Spaces. Some organizations provide a single, separate application for managing user credentials and prefer not to offer password management through other applications.

5. Use the **Profile Access** section to select which information sections display—**Summary**, **Employee**, **Business Contact**, **Personal Information**:
  - Select the **Available** check box to include a profile section.
  - Deselect the **Available** check box to exclude a profile section.
6. Specify whether WebCenter users can edit their profile details, section-by-section:
  - Select the **Can Edit** check box to allow users to edit a profile section.
  - Deselect the **Can Edit** check box to make a section read-only.
7. Use the **Profile Attributes** section to specify whether WebCenter users can modify individual profile attributes:
  - Select the **Allow Update** check box to allow users to update a profile attribute.
  - Deselect the **Allow Update** check box to make a particular profile attribute read-only.

Allow Update check box selections are only effective when the parent section is displayed and editable, that is, the **Available** and **Can Edit** check boxes must both be checked.

8. Click the **Apply** button to save your settings.

## 18.10 Enabling and Disabling WebCenter Services

In WebCenter Spaces, a series of WebCenter services expose social networking and personal productivity features and functionality through various task flows.

Table 18–2 lists the services available to WebCenter Spaces and groups them into three classifications: social networking, personal productivity, and intersecting services, which combine the first two.

**Table 18–2 WebCenter Services**

| Personal Productivity          | Intersecting           | Social Networking                                 |
|--------------------------------|------------------------|---|
| Mail <sup>1</sup>              | Documents <sup>1</sup> | Announcements <sup>1</sup>                        |
| Notes <sup>2</sup>             | Events <sup>2</sup>    | Blog <sup>1</sup>                                 |
| Recent Activities <sup>2</sup> | Links <sup>2</sup>     | Discussions <sup>1</sup>                          |
| RSS <sup>1</sup>               | Lists <sup>2</sup>     | Instant Messaging and Presence (IMP) <sup>1</sup> |
| Search <sup>1</sup>            | Page <sup>2</sup>      | Wiki <sup>1</sup>                                 |
| Worklist <sup>1</sup>          | Tags <sup>2</sup>      |   |

<sup>1</sup> Connection to external back-end required.

<sup>2</sup> Connection to WebCenter repository and MDS repository required (databases where notes, events, links, lists, pages, and tags are stored).

Some WebCenter services<sup>1</sup>, such as Mail, require an external back-end server. The Fusion Middleware Administrator is responsible for managing connections to all external servers and also maintains the WebCenter and MDS repositories<sup>2</sup> where application data, specific to WebCenter Spaces, is stored. See also [Chapter 3, "Maintaining WebCenter Spaces"](#).

When a service, such as Mail, is available in WebCenter Spaces:

- Associated task flows display in the resource catalog.
- Existing task flows function as expected.
- (Group space services only) Moderators choose whether to enable or disable the service in their group spaces—using the *Group Space Settings - Services* page.

When a back-end server is not configured, intentionally or otherwise, WebCenter Spaces cannot offer features or functionality related to that service:

- Associated task flows are not available in the resource catalog.
- Existing task flows display a message indicating that the service is currently unavailable.
- (Group space services only) Service is not listed, as available, to group space moderators —on *Group Space Settings - Services* page.

### Reporting Temporary Issues with WebCenter Services

When a service is temporarily unavailable, report the issue to the Fusion Middleware Administrator. The Fusion Middleware Administrator can use Fusion Middleware Control to investigate, diagnose, and solve issues with WebCenter services. See also, [Section 15.2.1, "Monitoring WebCenter Spaces"](#).

### Hiding Task Flows Belonging to Disabled Services

Most WebCenter Services are optional. If you decide not to offer a particular service in WebCenter Spaces, temporarily or permanently, consider removing any associated task flows that display, by default, out-of-the-box.

Oracle recommends that you hide disabled services in the sidebar too. See, [Section 18.3, "Customizing the Sidebar"](#).

### Enabling and Disabling Services for a Single Group Space

Group space moderators can enable or disable available WebCenter services within their group spaces. See, "Enabling and Disabling Services Available to a Group Space" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

## 18.11 Enabling and Disabling Personal Spaces

Personal spaces are optional in WebCenter Spaces—it is not mandatory to provide users with a private work area where they can store personal content and perform personal tasks. Users can fully participate in group space collaboration projects without a personal space.

Users who do not have a personal space are presented with My Group Spaces when they login. No personal productivity tools are available (such as the personal sidebar, favorites links, and so on) and users cannot create personal pages or see personal pages that other users might share.

The `Application-View` permission controls which users have their own personal space. Administrators can disable personal spaces for everyone using WebCenter Spaces or specific users only. Use the table in step 5 to determine which permission settings you require.

To enable or disable user access to personal spaces:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Security** tab.
4. Click the **Roles** tab.
5. Select or clear the **Application-View** check box as follows:

| Role            | Select Application-View   | Clear Application-View  |
|-----------------|---|---|
| Spaces-User     | Everyone has a personal space.                                      | Users do not have a personal space unless you grant them another role that specifies otherwise. |
| Any Custom Role | Users assigned any custom role have a personal space.               | Users with this role do not have a personal space. <sup>1</sup>                                 |
| Administrator   | Users assigned this role have a personal space.                     | Users with this role do not have a personal space. <sup>1</sup>                                 |
| Public-User     | Unauthenticated users can see personal pages/content marked public. | Unauthenticated users only see the login page.  |

<sup>1</sup> Assumes the Application-View permission is disabled for the Spaces-User and the Public-User.

6. Click **Apply** to save.

New permissions are effective immediately.

## 18.12 Publishing the WebDAV URL

WebCenter Spaces uses an Oracle Content Server to store group space and personal space documents. WebDAV (Web-Based Distributed Authoring and Versioning),



which allows users to look at their content repository using their Windows Explorer, can be used with Oracle Content Server and hence with WebCenter Spaces content.

Using WebDAV, WebCenter users can seamlessly drag and drop content, files, and folders back and forth between their desktop and their personal and group spaces. Users will not know the WebCenter Spaces WebDAV URL for unless you publish this information—maybe in a document or on a business role page that everyone can access.

Contact your Fusion Middleware Administrator to find out the URL for the Oracle Content Server that WebCenter Spaces is using to store group space and personal space documents. If the base URL for that Oracle Content Server is `http://<host>:<port>/<relative_web_root>`, the WebDAV root URL will be `http://<host>:<port>/<relative_web_root>/idcplg/webdav`.

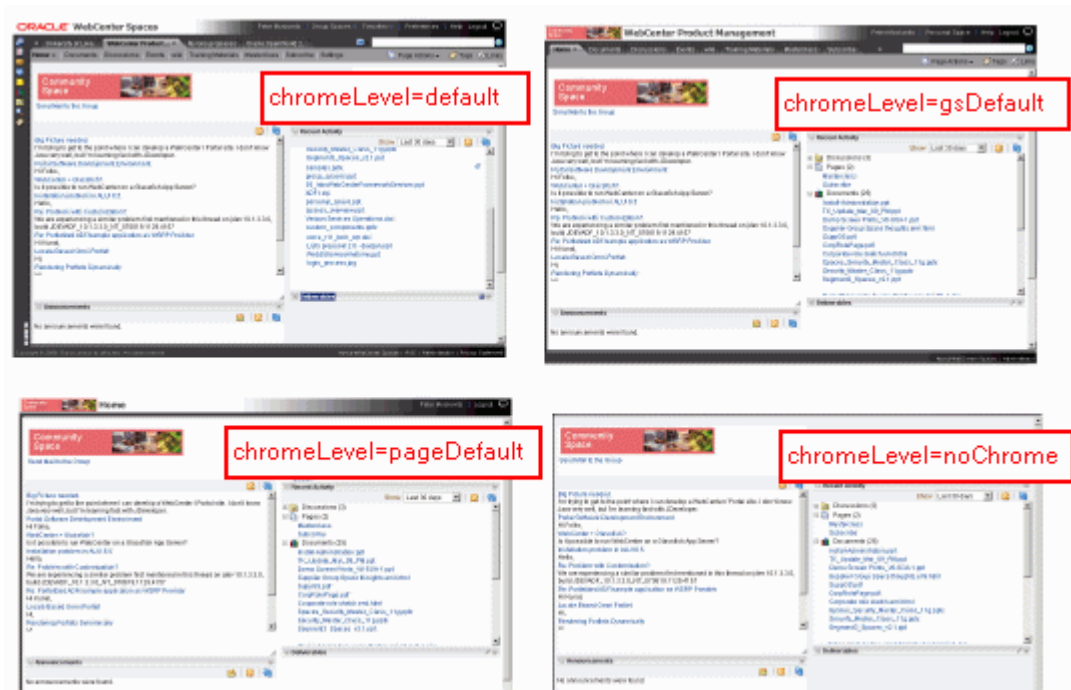
## 18.13 Overriding and Customizing Application Templates

A series of application templates define what is displayed around WebCenter pages. For example, application templates define areas such as the global tool bar, the sidebar, the footer, and so on (Figure 18–11).

Out-of-the-box application templates include:

- **default** - Normal WebCenter Spaces view with global tool bar, the sidebar, the footer, and so on.
- **gsDefault** - Group space full-screen mode.
- **pageDefault** - Page full-screen mode
- **tabLess** - Default WebCenter Spaces view without any tabs.
- **noChrome** - Print preview mode.

Figure 18–11 Application Templates - chromeLevel Options





Users can view any page with any one of these application templates by appending a URL parameter called `wc.chromeLevel` to the page's URL. For example:  
`http://mycompany.com/webcenter/spaces/mygroup/page/Contacts?wc.chromeLevel=noChrome`.

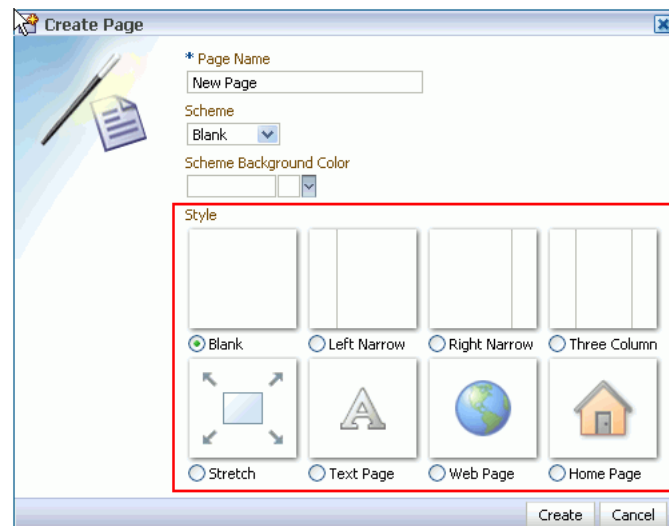
If you want to exclude certain content or display different content within these template areas you must modify the default application templates through JDeveloper. Custom application template deployment typically takes place *before* the WebCenter Spaces application goes live or during scheduled maintenance periods as the application's managed server must be restarted for changes to take effect.

For more information, refer to the whitepaper entitled "*Extending WebCenter Spaces*" available on the Oracle Technology Network (<http://webcenter.oracle.com>).

## 18.14 Making New Page Styles Available

WebCenter Spaces offers eight page styles out-of-the-box (Figure 18–12).

**Figure 18–12 Standard Page Styles**



Some page styles come prepopulated with a selection of useful task flows. Others include properties that suggest a particular use for the page. For example, the Web page style includes a configurable property for specifying a URL. See "WebCenter Seeded Page Styles" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

If the built-in page styles do not suit your requirements or you want to offer a different set of page styles, you may create page styles of your own (defined in jsp files) and deploy them to WebCenter Spaces.

Newly deployed page styles only become available to WebCenter Spaces once the application's managed server is restarted, so custom page styles are typically deployed before the WebCenter Spaces application goes live or during scheduled maintenance periods.

For more information, refer to the whitepaper entitled "*Extending WebCenter Spaces*" available on the Oracle Technology Network (<http://webcenter.oracle.com>).

## 18.15 Customizing the Resource Catalog and Deploying New Task Flows

In WebCenter Spaces, the Oracle Composer's catalog provides access to page content, such as task flows and portlets, and page layout components, such as images, content boxes, hyperlinks, and the like. The catalog presents available resources in a series of folders and subfolders and the content on offer changes dynamically depending on which services are currently available. For example, in a particular group space, mail-related task flows will display in the group space catalog when mail services are available but will not display if the back-end mail server is not yet configured or the Mail service has been disabled by the group space moderator.

WebCenter Spaces provides two catalogs out-of-the-box—a personal space catalog and a group space catalog. Each catalog contains a default set of task flows. Should you need to add new task flows, remove task flows, or reorganize the folder hierarchy to better suit your audience you can make a copy, and customize each catalog through JDeveloper.

Resource catalog customization and new task flow deployment typically take place before the WebCenter Spaces application goes live or during scheduled maintenance periods as the application's managed server must be restarted for the changes to take effect.

For more information, refer to the whitepaper entitled "*Extending WebCenter Spaces*" available on the Oracle Technology Network (<http://webcenter.oracle.com>).

---

# Managing Users and Roles for WebCenter Spaces

This chapter describes how to manage users, roles, and permissions in WebCenter Spaces. It includes the following sections:

- [Understanding Users, Roles, and Permissions](#)
- [Managing Users](#)
- [Managing Application Roles and Permissions](#)
- [Allowing Self-Registration](#)

## Audience

The content of this chapter is intended for WebCenter Spaces administrators. Users granted the WebCenter Spaces Administrator role or a custom role that grants the Application-Manage permission).

Refer to [Chapter 14, "Managing Security"](#) if you are a Fusion Middleware Administrator responsible for security-sensitive administrative duties that require configuration through Fusion Middleware Control or WLST.

## 19.1 Understanding Users, Roles, and Permissions

Read this section to understand more about WebCenter users, application roles, and permissions granted to WebCenter users working in their personal space. It includes the following subsections:

- [Managing Users](#)
- [Understanding Application Roles](#)
- [Understanding Application Permissions](#)
- [Understanding Discussions Server Role and Permission Mapping](#)

When a WebCenter user becomes a member of a group space, a different set of roles and responsibilities apply. See "What You Should Know About Group Space Roles and Permissions" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

### 19.1.1 Understanding Users

A WebCenter user is a member of WebCenter Spaces—provisioned directly from an existing identity store. See also, [Section 14.3, "Configuring the Identity Store"](#).

All users in the identity store are assigned minimal WebCenter Spaces privileges through the Spaces-User role. The only exception is the Fusion Middleware

Administrator (`weblogic`). Out-of-the-box, the Fusion Middleware Administrator is the only user assigned full administrative privileges through the Administrator role. For more information, read the next section [Section 19.1.2.1, "Default Application Roles"](#).

It is the Fusion Middleware Administrator's job to assign each WebCenter user an appropriate application role. Alternatively, the Fusion Middleware Administrator may choose to assign the Administrator role to another user and delegate this responsibility.

**Table 19–1 Default Administrator in WebCenter Spaces**

| User  | Description  |
|---|--|
| Fusion Middleware Administrator ( <code>weblogic</code> ) | Administrator for the entire application server, sometimes referred to as the super administrator. This user can manage any application on the server, including WebCenter Spaces. |

WebCenter Spaces supports self-registration. When new WebCenter users self-register, they create their own login and password and a new user account is created in the identity store. See also, [Section 19.4, "Allowing Self-Registration"](#).

## 19.1.2 Understanding Application Roles

Application roles control the level of access a user has to information and services in WebCenter Spaces. Specifically, application roles determine what a user can see and do in their *personal space*.

Application role assignment is the responsibility of the WebCenter Spaces administrator. Administrators can assign users one of the default application roles or create additional, custom roles specific to their WebCenter Spaces application. For more detail, see:

- [Default Application Roles](#)
- [Custom Application Roles](#)

Application roles only apply while a user is working within their personal space. Within a particular group space a different set of roles and permissions apply and it is the group space moderator's responsibility to determine suitable role assignments for each of its members. See also "Managing Group Space Roles and Permissions" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

---

**Note:** Application roles and permissions defined within WebCenter Spaces are stored in its *policy store* and, consequently, apply to this WebCenter Spaces application only. Enterprise roles are different; enterprise roles are stored within the application's *identity store* and do not imply any permissions within WebCenter Spaces.

---

### 19.1.2.1 Default Application Roles

WebCenter Spaces provides several default application roles that cannot be deleted ([Table 19–2](#)).

**Table 19–2 Default Application Roles for WebCenter Spaces**

| Application Role | Description  | Modify?  |
|------------------|--|--|
| Administrator    | <p>Users with the <code>Application-Manage</code> permission. Anyone with the <code>Administrator</code> role can set application-wide properties for WebCenter Spaces, configure defaults for discussion forums and personal profiles, create business role pages, and perform other administrative duties.</p> <p>Administrators can also manage users and roles for WebCenter Spaces, delegate or revoke privileges to/from other users, manage group spaces and group space templates, as well as import and export group space information.</p> <p>Out-of-the-box, the Fusion Middleware Administrator is the only user assigned full WebCenter Spaces administrative privileges through the <code>Administrator</code> role.</p> | <p>Yes*</p> <p>*Except for Application permissions which are read-only</p> |
| Spaces-User      | <p>Authenticated users of WebCenter Spaces are granted the <code>Spaces-User</code> role. Once logged in, users assigned with this role have access to their own personal space, pages that they create, and public pages. These users can also view public group spaces, create group spaces, and create group space templates.</p> <p>This role inherits permissions from the <code>Public-User</code> role.</p> <p>In WebCenter Spaces, the <code>Spaces-User</code> role is equivalent to the <code>authenticated-user</code> role.</p>  | Yes  |
| Public-User      | <p>Anyone with access to WebCenter Spaces who is not logged in, is granted the <code>Public-User</code> role. Such users are anonymous, unidentified, and can see public content only.</p> <p>In WebCenter Spaces, the <code>Public-User</code> role is equivalent to the <code>anonymous-role</code>.</p>   | Yes  |

### 19.1.2.2 Custom Application Roles

Custom application roles (sometimes known as user-defined roles) are specific to your WebCenter Spaces application. When setting up WebCenter Spaces, it is the WebCenter Spaces administrator's job to identify which application roles are required, choose suitable role names, and define the responsibilities of each role.

For example, an education environment might require roles such as Teacher, Student, and Guest. While roles such as Finance, Sales, Human Resources, and Support would be more appropriate for a corporate environment.

To learn how to set up applications roles for WebCenter users, see [Section 19.3.2, "Defining Application Roles."](#)

## 19.1.3 Understanding Application Permissions

Every application role has specific, defined capabilities known as permissions. These permissions allow individuals to perform specific actions in their personal space. Permissions are categorized as follows and listed individually in the subsequent tables:

- Application
- Group Spaces

- Group Space Templates
- Pages
- Discussions
- Links
- Profile Management

With a particular category, the **Manage** permission (such as `Group Spaces-Manage`) contains all other permissions (for example, `Group Spaces-Configure` and `Group Spaces-View`). No permission, except **Manage**, inherits privileges from other permissions.

**Table 19-3 Application Permissions in WebCenter Spaces**

| Category              | Application Permissions   |
|-----------------------|---|
| Application           | <p><b>Manage</b> - Manage security, application-wide properties, services, personal pages, and business role pages.</p> <p><b>Configure</b> - Manage application-wide properties, services, personal pages, and business role pages.</p> <p><b>View</b> - View the WebCenter Spaces application.</p>  |
| Group Spaces          | <p><b>Manage</b> - Manage group space membership and assign permissions and roles. Manage, delete, and export all group spaces. Create group space content, set properties, and manage service availability.</p> <p><b>Configure</b> - Manage, delete, and export all group spaces. Contribute to group spaces, for example, add pages, content, post discussion forum topics, add list items, upload documents. Set group space properties, and manage service availability.</p> <p><b>View</b> - View group space information.</p> <p><b>Create</b> - Create group spaces.</p>  |
| Group Space Templates | <p><b>Manage</b> - Manage and delete all group space templates. Export group space templates.</p> <p><b>View</b> - View group space template information. Create group spaces based on a template.</p> <p><b>Create</b> - Create group space templates.</p>   |
| Pages                 | <p><b>Manage</b> - Edit properties of a personal page, set personal page permissions, and all other page actions.</p> <p><b>Delete</b> - Delete a personal page.</p> <p><b>Edit</b> - Add or edit personal page content, rearrange content, and set page parameters and properties.</p> <p><b>Personalize</b> - Personalize your view of a personal page by adding, editing, or removing content.</p> <p><b>View</b> - View a personal page.</p> <p><b>Create</b> - Create or design a new personal page.</p> <p>These permissions do not apply to group space pages. Group space page permissions are granted on a per group space-basis by the group space moderator.</p> |

**Table 19–3 (Cont.) Application Permissions in WebCenter Spaces**

| Category           | Application Permissions  |
|--------------------|--|
| Discussions        | <b>Manage</b> - Manage categories, forums, and topics on the back-end discussions server. Set discussion forum properties for all group spaces. See also, <a href="#">Section 19.1.4, "Understanding Discussions Server Role and Permission Mapping"</a> . |
| Links              | <b>Manage</b> - Create and delete links between objects, and manage link permissions.<br><b>Delete</b> - Delete a link between two objects.<br><b>Create</b> - Create links between objects.   |
| Profile Management | <b>Manage</b> - Configure profile data display options. Enable profile data and WebCenter password updates.<br><b>Edit</b> - Edit your own profile data.   |

### 19.1.4 Understanding Discussions Server Role and Permission Mapping

WebCenter Spaces uses *application roles* to manage user permissions in personal spaces and *group space roles* to manage user permissions with a group space. On the Oracle WebCenter Discussions server, a different set of roles and permissions apply.

Users who are working with discussions and announcements in WebCenter Spaces automatically map to the appropriate Oracle WebCenter Discussions server role, see [Table 19–4](#) and [Table 19–5](#).

**Table 19–4 Discussions Server Roles and Permissions - Application**

| Discussion Server Role | Discussion Server Permissions | WebCenter Spaces Equivalent Application Permission   |
|------------------------|-------------------------------|--|
| Administrator          | Category Admin                | Discussions-Manage<br>Create, read, update and delete sub categories, forums and topics inside the category for which permissions are granted. |

**Table 19–5 Discussions Server Roles and Permissions - For Group Spaces**

| Discussion Server Role | Discussion Server Permissions | WebCenter Spaces Equivalent Group Space Permissions  |
|------------------------|-------------------------------|--|
| Moderator              | Category Admin                | <ul style="list-style-type: none"> <li>■ Discussions-Manage<br/>Create, read, update and delete forums and topics.</li> <li>■ Announcements-Manage<br/>Create, read, update and delete announcements.</li> </ul> |
|                        | Forum Admin                   |  |
|                        | Read Forum                    | <ul style="list-style-type: none"> <li>■ Discussions-Edit<br/>Create and reply to topics.</li> <li>■ Announcements-Edit<br/>Create and edit announcements.</li> </ul>  |
|                        | Create Thread                 |  |
|                        | Create Message                |  |
|                        | Create Announcement           |  |
|                        | Read Forum                    | <ul style="list-style-type: none"> <li>■ Discussions-View<br/>View forums and topics.</li> <li>■ Announcements-View<br/>View announcements.</li> </ul>   |
|                        |                               |  |

Any user assigned the `Application-Discussions-Manage` permission in WebCenter Spaces is automatically added to Oracle WebCenter Discussions and assigned the `Administrator` role with the `Category Admin` permission. Out-of-the-box, WebCenter Spaces assigns the `Application-Discussions-Manage` permission to the `Administrator` role only, as shown in [Figure 19-1](#).

**Figure 19-1 Application Roles - Default Discussion Permissions**

| Permissions | Roles                               |                          |                          |
|-------------|-------------------------------------|--------------------------|--------------------------|
|             | Administrator                       | Spaces-User              | Public-User              |
| Discussions |                                     |                          |                          |
| Manage      | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Similarly, in group spaces, any member assigned the `Discussions-Manage`, `Discussions-Edit`, or `Discussion-View` permission is granted the corresponding permissions on the Oracle WebCenter Discussions server. Out-of-the-box, discussion and announcement permissions for the default group space roles `Moderator`, `Participant`, and `Viewer`, are as shown in [Figure 19-2](#).

**Figure 19-2 Group Space Roles - Default Discussion Permissions**

**Manage Group Space Roles**  
Group space roles determine what your members can see and do in the group space. Select or clear the check boxes to configure role permissions or click `Create Role` to define a new role for this group space.

| Permissions   | Roles                               |                                     |                                     |
|---------------|-------------------------------------|-------------------------------------|-------------------------------------|
|               | Moderator                           | Participant                         | Viewer                              |
| Announcements |                                     |                                     |                                     |
| Manage        | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/>            |
| Edit          | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |
| View          | <input type="checkbox"/>            | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |
| Discussions   |                                     |                                     |                                     |
| Manage        | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/>            |
| Edit          | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |
| View          | <input type="checkbox"/>            | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |

## 19.2 Managing Users

Administrators must ensure that all WebCenter users have appropriate permissions. To get permissions, users must be assigned to an appropriate application role.

This section tells you how to assign roles and contains the following subsections:

- [What You Need to Know About Managing Users](#)
- [Assigning Users to Roles](#)
- [Assigning a User to a Different Role](#)
- [Giving a User Administrative Privileges](#)
- [Revoking Application Roles](#)
- [Adding or Removing Users](#)

### 19.2.1 What You Need to Know About Managing Users

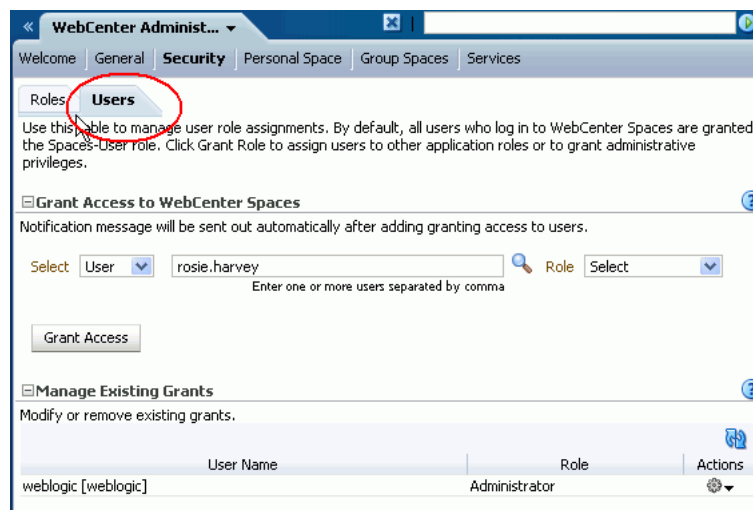
From the `Users` page ([Figure 19-3](#)), administrators can manage application roles for all the users who have access to WebCenter Spaces, that is, all users defined in the identity store. From here, you can change user role assignments, grant administrative privileges, and revoke user permissions.



Only users granted special (non-default) application privileges will appear in this table. Initially, all users in the WebCenter Spaces identity store are assigned minimal privileges through the Spaces-User role. Users with the default Spaces-User role are not listed here.

See also, [Section 14.3, "Configuring the Identity Store"](#).

**Figure 19–3 WebCenter Administration - Users Page**



## 19.2.2 Assigning Users to Roles

Initially, all users in the WebCenter Spaces identity store are assigned minimal privileges through the Spaces-User role.

To assign a user to a different application role:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Security** tab.
4. Click the **Users** tab ([Figure 19–3](#)).

This page lists WebCenter users to which additional roles are defined.

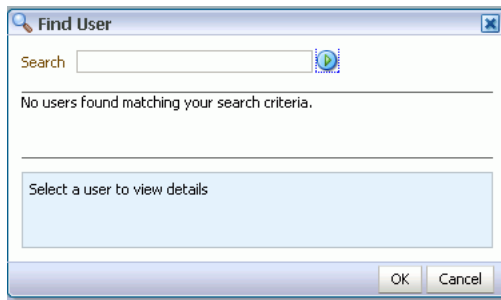
5. Choose **User** or **Group** from the drop down.  
Select **User** to grant permissions to one or more users defined in the identity store.  
Select **Group** to grant permissions to groups of users.
6. If you know the exact name of the user or group, enter the name in the box provided, separating multiple names with a comma.  
If you are not sure of the name you can search your identity store:
  - a. Click the **Find User** icon ([Figure 19–4](#)).

**Figure 19–4 Find User Icon**



The Find User dialog box opens (Figure 19-5).

**Figure 19-5 Finding Users and Groups in the identity store**



- b. Enter two or more characters that appear in the name you are looking for.
- c. Click the Search icon.
- d. Select one or more names from the list.
- e. Click OK.

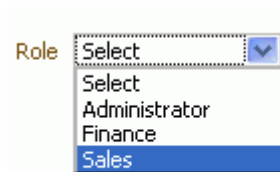
Users (or groups) matching your search criteria display in the **Select User** dialog box. The search is case-sensitive.

To assign roles to multiple users, multi-select all the names required. **Ctrl-Click** rows to select more than one.

The names that you select are display on the Users tab.

- 7. To assign a role, select a **Role** from the drop down (Figure 19-6).

**Figure 19-6 Assigning a User Role**



Select an appropriate role for the selected users (or groups). Only choose **Administrator** to assign full, administrative privileges for WebCenter Spaces.

If the role you want is not listed, create a new role that meets your requirements (see Section 19.3.2, "Defining Application Roles").

When no role is selected, the user assumes the `Spaces-User` role. See Section 19.1.2.1, "Default Application Roles".

- 8. Click **Grant Access**.

User's names and new role assignment display in the table.

### 19.2.3 Assigning a User to a Different Role

From time to time, a user's role in WebCenter Spaces may change. For example, a user may move out of sales into the finance department and in this instance, the user's role assignment might need to change from *Sales* to *Finance*.

---

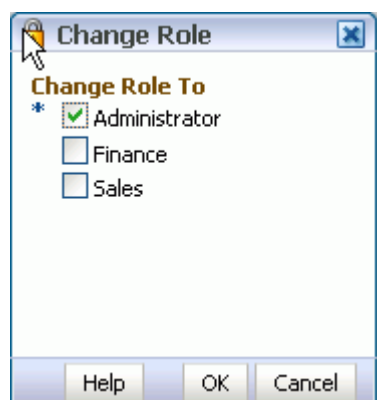
**Note:** You cannot modify your own role or the Fusion Middleware Administrator's role. See [Section 19.1.2, "Understanding Application Roles"](#).

---

To assign a user to a different role:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Security** tab.
4. Click the **Users** tab.
5. In the **Manage Existing Grants** table, scroll down to the user you want.  
Only users with non-default role assignments are listed in the table. If the user you want is not listed, grant the role required as described in [Section 19.2.2, "Assigning Users to Roles"](#).
6. Click the **Actions** icon, then choose **Change Role** from the drop down list.  
The Change Role dialog box opens ([Figure 19–7](#)).

**Figure 19–7** *Changing a User's Application Role*



7. Select roles as follows:
  - Select **Administrator** to assign full, administrative privileges for WebCenter Spaces.
  - Select select one or more roles from the list available.

If the role you want is not listed, create a new role that meets your requirements (see [Section 19.3.2, "Defining Application Roles"](#)).

At least one role must be selected. To revoke all role assignments, reverting user permissions to the default Spaces-User role, see [Section 19.2.5, "Revoking Application Roles"](#).
8. Click **OK**.

New role assignments display in the table.

## 19.2.4 Giving a User Administrative Privileges

It is easy to give a user full, administrative privileges for WebCenter Spaces through the Administrator role. Administrators have the highest privilege level and can view and modify anything in WebCenter Spaces so take care when assigning the Administrator role.

To give a user administrative privileges:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).

2. Click the **Administration** link at the top of the application.

3. Click the **Security** tab.

4. Click the **Users** tab.

The Role column indicates which users already have full administrative privileges through the Administrator role.

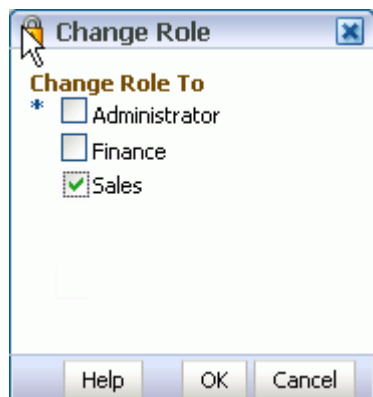
5. In the **Manage Existing Grants** table, scroll down to the user you want.

Only users with non-default role assignments are listed in the table. If the user you want is not listed, follow steps in [Section 19.2.2, "Assigning Users to Roles"](#) to grant the Administrator role.

6. Click the **Actions** icon, then choose **Change Role** from the drop down list.

The Change Role dialog box opens ([Figure 19–7](#)).

**Figure 19–8 Changing a User's Application Role**



7. Select **Administrator** to assign full, administrative privileges for WebCenter Spaces.

8. Select **OK**.

The new role assignment displays in the table.

## 19.2.5 Revoking Application Roles

It is easy to revoke application role assignments that no longer apply. You can revoke roles individually or revoke all application roles assigned to a particular user at once.

Revoking all a user's application roles does not remove that user from the identity store and the user still has access to WebCenter Spaces through the default Spaces-User role.

---

---

**Note:** You cannot revoke your own role assignments or the Fusion Middleware Administrator's role. See [Section 19.1.2, "Understanding Application Roles"](#).

---

---

To revoke application roles:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Security** tab.
4. Click the **Users** tab.
5. In the **Manage Existing Grants** table, scroll down to the user you want.
6. Click the **Actions** icon:
  - Choose **Change Role** icon to revoke one or more, specific application roles. See also [Section 19.2.3, "Assigning a User to a Different Role"](#).
  - Choose **Delete Role Assignments** to revoke all roles assigned to that user, and then click **Delete** when asked for confirmation.

Access for that user is revoked immediately.

When you delete all the roles assigned to a particular user, the user is no longer listed on the Users page. The user remains in the identity store and still has access to WebCenter Spaces through the Spaces-User role. See [Section 19.1.2.1, "Default Application Roles"](#).

## 19.2.6 Adding or Removing Users

WebCenter Spaces administrators cannot add new user data directly to the WebCenter Spaces identity store or remove user credentials. Identity store management is the responsibility of the systems administrator and takes place through the WLS Administration Console or directly into embedded LDAP identity stores using LDAP commands. See also, [Section 14.3.3, "Adding Users to the Identity Store"](#).

WebCenter Spaces administrators can, however, enable self-registration for the application. Through self-registration, invited and uninvited users can create their own login and password for WebCenter Spaces. A user who self registers is immediately and automatically granted access to WebCenter Spaces and a new user account is created in the identity store. See also, [Chapter 19.4, "Allowing Self-Registration"](#).

## 19.3 Managing Application Roles and Permissions

WebCenter Spaces uses application roles to manage permissions for users working in their *personal space*. This section tells you how to manage application roles, and their permissions from WebCenter Administration pages. It contains the following subsections:

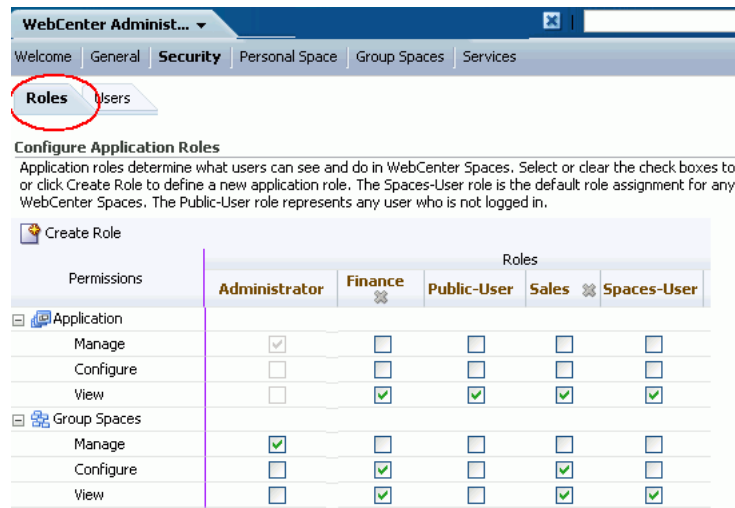
- [What You Need to Know About Application Roles and Permissions](#)
- [Defining Application Roles](#)
- [Modifying Application Role Permissions](#)

- [Granting Permissions to the Public-User](#)
- [Granting Permissions to the Spaces-User](#)
- [Deleting Application Roles](#)

### 19.3.1 What You Need to Know About Application Roles and Permissions

From the Roles page (Figure 19–9), administrators can manage application roles and permissions. From here, you can edit the permissions assigned to an application role, create new application roles, or delete unused roles.

**Figure 19–9 WebCenter Administration - Roles Page**



Application roles apply when a user is working within their personal space. A different set of roles and permissions apply when a user is working within a particular group space. It is the group space moderator's responsibility to determine suitable role assignments for each of its group space members. See also "Managing Group Space Roles and Permissions" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

WebCenter Spaces provides several default application roles. You cannot delete default application roles but you can modify the default permission assignments for each role. For more information, see [Section 19.1, "Understanding Users, Roles, and Permissions"](#).

### 19.3.2 Defining Application Roles

Use roles to characterize groups of WebCenter users and determine what they can see and do in their personal spaces.

When defining application roles, use self-descriptive role names and try to keep the role policy as simple as possible. Choose as few roles as you can, while maintaining an effective policy.

Take care to assign appropriate access rights when assigning permissions for new roles. Do not allow users to perform more actions than are necessary for the role but at the same time, try not to inadvertently restrict them from activities they must perform. In some cases, users might fall into multiple roles.

To define a new application role:

1. Login to WebCenter Spaces with administrative privileges.

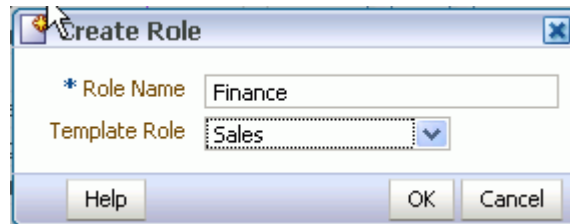
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).

2. Click the **Administration** link at the top of the application.
3. Click the **Security** tab.
4. Click the **Roles** tab.

Current application roles for WebCenter Spaces display as columns in the table.

5. Click **Create Role** to define a new role for WebCenter users.

**Figure 19–10** *Creating a New Role*



6. Enter a suitable name for the role.

Ensure the role names that are self-descriptive. Make it as obvious as possible which users should belong to which roles. Role names cannot include special characters or whitespace.

7. (Optional) Choose a **Template Role**.

The new role inherits permissions from the template role. You can modify these permissions in the next step.

Choose **Administrator** to create a role that inherits full, administrative privileges. Conversely, choose `Public-User` to create a role that *typically* provides minimal privileges. Alternatively, choose one of the custom application roles to be your template.

8. Click **OK**.

The new role appears as a column in the table. The permissions list shows which actions users with this role can perform.

9. To modify user permissions for the role, select or clear each permission check box.
10. Click **Apply** to save any changes that you make to the role's permissions.

### 19.3.3 Modifying Application Role Permissions

Administrators can modify the permissions associated with application roles at any time. Application permissions are described in [Section 19.1.3, "Understanding Application Permissions"](#).

Application role permissions allow individuals to perform specific actions in their personal space. With a particular category, the `Manage` permission (such as `Group Spaces-Manage`) contains all other permissions (for example, `Group Spaces-Configure` and `Group Spaces-View`).

---

**Note:** Application permissions cannot be modified for the `Administrator` role. See also [Section 19.1.2.1, "Default Application Roles"](#).

---

To change the permissions assigned to a role:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Security** tab.
4. Click the **Roles** tab.
5. Select or clear **Permissions** check boxes to enable or disable permissions for a role.
6. Click **Apply** to save.

The new permissions are effective immediately.

### 19.3.4 Granting Permissions to the Public-User

Anyone who is not logged in to WebCenter Spaces assumes the `Public-User` role. Out-of-the-box, the `Public-User` role is granted minimal privileges, that is, the `Application-View` permissions only.

---

---

**Caution:** Take care when granting permissions to the `Public-User` role. Avoid granting administrative permissions such as `Application-Manage`, `Application-Configure`, other `Manage` permissions, or any permission that might be considered unnecessary.

---

---

#### Granting the Application-View Permission

The `Application-View` permission allows unauthenticated users to see public WebCenter Spaces application pages, such as the welcome page, as well as content that individual WebCenter users choose to make public.

When `Application-View` permissions are granted to the `Public-User` role:

- Ensure that your WebCenter users understand that any personal page or personal content they choose to make public will become accessible to unauthenticated users outside of the WebCenter Spaces community, that is, anyone with Web access.
- Consider customizing the default welcome page that displays to public users before they login. See [Section 20.3.1, "Customizing the Public Welcome Page"](#).

If you do not want unauthenticated users to see WebCenter Spaces content that is marked 'public', do not grant the `Application-View` permission to the `Public-User` role. When public access is disabled, public content cannot be seen by unauthenticated users. Also, the welcome page for WebCenter Spaces is not displayed; public users are directed straight to a login page. Administrators may customize the default login page, if required. See [Section 20.3.2, "Customizing the Login Page"](#).

#### Granting Other Permissions

Be careful when assigning permissions to the `Public-User` role. For security reasons, Oracle recommend that you limit what anonymous users can see and do in WebCenter Spaces.

### 19.3.5 Granting Permissions to the Spaces-User

Anyone who is logged in to WebCenter Spaces assumes the `Spaces-User` role. Out-of-the-box, the `Spaces-User` role is granted minimal privileges, that is, the



Application-View, Group Space-Create, Group Space Templates-Create, Pages-Create, Profiles-Edit permissions only.

Note that the Spaces-User role always inherits permissions from the Public-User role.

### 19.3.6 Deleting Application Roles

When an application role is no longer required you should remove it from WebCenter Spaces. This helps maintain a valid role list, and prevents inappropriate role assignment.

Application roles are deleted even when users are still assigned to the them. As you cannot delete any default roles, WebCenter users will always have the Spaces-User role.

---

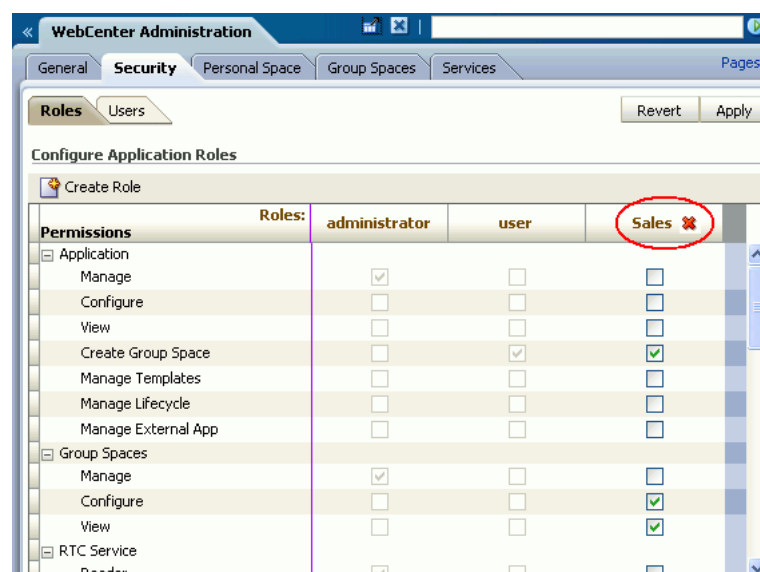
**Note:** Default roles cannot be deleted (Administrator, Spaces-User, Public-User). See [Section 19.1.2.1, "Default Application Roles"](#).

---

To delete an application role:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Security** tab.
4. Click the **Roles** tab.
5. Select the Delete Role icon next to the role you want to delete ([Figure 19–11](#)).

**Figure 19–11 Deleting an Application Role**



6. Click **OK** to confirm that you want to delete the role.  
The role is removed from the table. Any users assigned to this role only, assume the default Spaces-User role and do not display on the Users tab.

## 19.4 Allowing Self-Registration

Self-registration allows users to create their own login and password for WebCenter Spaces. A user who self registers is immediately and automatically granted access to WebCenter Spaces and a new user account is created in the application's identity store.

When *anyone* is allowed to self-register, that is any public user, a Register link or Register button displays below the WebCenter Spaces login form. To enable this feature, see [Section 19.4.2, "Enabling Anyone to Self-Register"](#).

Self-registration by invitation is allowed too. This feature allows group space moderators to send out membership invitations to people who are not currently registered with WebCenter Spaces but might be interested in their group space. Before accessing the group space, invitees must create an account with WebCenter Spaces and their account details are added to the application's identity store. When the group space moderator approves their subscription request they will gain access to the group space. See [Section 19.4.1, "Enabling Self-Registration By Invitation-Only"](#).

---

---

**Note:** If self-registration is not enabled in WebCenter Spaces, identity store management takes place through the WLS Administration Console (or directly into embedded LDAP identity stores using LDAP commands) and is the responsibility of your systems administrator. See also, [Section 14.3.3, "Adding Users to the Identity Store"](#).

---

---

A self-registration page is supplied out-of-the-box. Administrators can add new components to the page and change the page layout if required. See [Section 20.3.3, "Customizing the Self-Registration Page"](#).

The self-registration page provided with WebCenter Spaces offers to send a "user name reminder email" to anyone who tries to register using an existing email address. This feature only works if public credentials are defined for the external application that is providing authentication for the Mail service. If users experience issues with this feature, ask your Fusion Middleware Administrator to check the mail server connection and its associated external application connection are configured correctly and that public credentials are defined. See also, [Section 11.3.3, "Registering Mail Servers"](#).

### 19.4.1 Enabling Self-Registration By Invitation-Only

Out-of-the-box, only existing WebCenter users are candidates for group space membership. While this might meet the needs of most WebCenter Spaces applications it is likely that some group spaces will want to recruit members outside of the WebCenter Spaces community.

The WebCenter Spaces administrator can extend group space membership to users outside of WebCenter Spaces by allowing them to self-register on an *invitation-only* basis. When this facility is enabled, group space moderators can invite anyone to join their group space by sending them a customizable invitation by mail. The invitation includes a secure, self-registration URL which the invited party clicks to accept group space membership.

New members recruited in this way must create an account with WebCenter Spaces before gaining access to the group space. Users who self-register by invitation are added to the identity store, and to the group space member list.

---

**Note:** Users who self-register by invitation will be assigned the default application role too—`Spaces-User`. Out-of-the box, users with the `Spaces-User` role have access to their own personal space, pages that they create, and public pages. They are also allowed to view public group spaces, join any group space that allows self-subscription, and create group spaces of their own. When you enable self-registration, consider modifying `Spaces-User` permissions to suit your exact requirements. See also, [Section 19.3.3, "Modifying Application Role Permissions"](#).

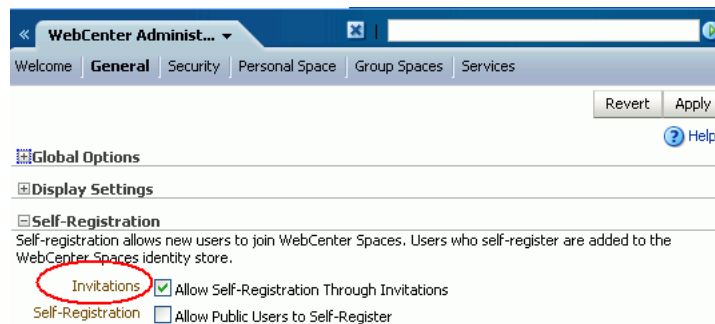
---

To allow external users to join group spaces:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **General** tab.
4. Select **Allow Self-Registration Through Invitations** ([Figure 19–12](#)).

When you deselect this option, only existing WebCenter users are candidates for group space membership.

**Figure 19–12 Allowing Self-Registration Through Invitations**



5. Click **Apply**.

Group space moderators may invite non-WebCenter users to become members of their group space. See "Inviting a Non-WebCenter Spaces User" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

## 19.4.2 Enabling Anyone to Self-Register

When *anyone* is allowed to self-register, that is any public user, a Register link displays in the top right corner of the application or a Register button displays below the WebCenter Spaces login form ([Figure 19–13](#)).

**Figure 19–13 Self-Registration Available on Login Form**



New users must create an account before gaining access to the WebCenter Spaces application.

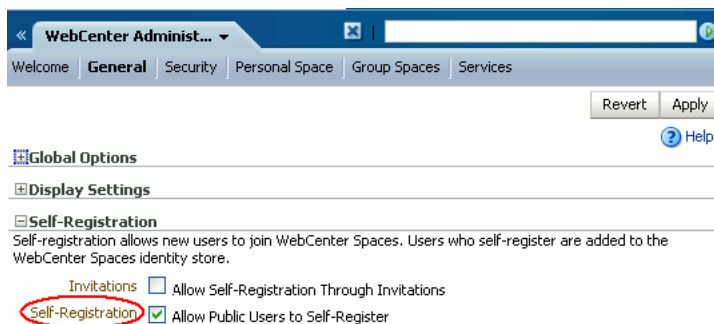
Users who self-register are added directly to the WebCenter Spaces identity store and assigned the `Spaces-User` application role. Out-of-the-box, users with `Spaces-User` role have access to their own personal space, pages that they create, and public pages. They are also allowed to view public group spaces, join any group space that allows self-subscription, and create group spaces of their own. If you enable self-registration, consider modifying `Spaces-User` permissions to suit your exact requirements. See [Section 19.3.3, "Modifying Application Role Permissions"](#).

To allow anyone to self-register with WebCenter Spaces:

1. Log in to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **General** tab.
4. Select **Allow Public Users to Self-Register** ([Figure 19–14](#)).

When you deselect this option, public users cannot self-register with WebCenter Spaces. You still enable self-registration on an invitation-only basis if you want. See [Section 19.4.1, "Enabling Self-Registration By Invitation-Only"](#).

**Figure 19–14 Allowing Self-Registration Through Invitations**



5. Click **Apply**.

See also, "Registering Yourself with WebCenter Spaces" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.



---

---

## Managing Pages in WebCenter Spaces

This chapter describes how to manage personal pages and business role pages, and how to set up WebCenter Spaces for the public user. It includes the following sections:

- [Managing Business Role Pages](#)
- [Managing Personal Pages](#)
- [Setting Up the Public User Experience](#)

### Audience

The content of this chapter is intended for WebCenter Spaces administrators. Users granted the WebCenter Spaces Administrator role or a custom role that grants the Application-Manage permission).

## 20.1 Managing Business Role Pages

- [What You Should Know About Business Role Pages](#)
- [Creating a Business Role Page](#)
- [Specifying the Target Audience for Business Role Pages](#)
- [Choosing a Default Display Order for Business Role Pages](#)
- [Editing a Business Role Page](#)
- [Copying a Business Role Page](#)
- [Deleting a Business Role Page](#)

### 20.1.1 What You Should Know About Business Role Pages

A business role page is different to a personal page in that it gets *pushed* to all the users to which it is assigned. When a user logs in, they immediately see business role pages assigned to them as a tab in their personal space. Personal pages are not presented automatically to others when shared. Users discover personal pages that others have shared through their page manager.

Business role pages are an efficient way of rolling out pages to a common audience. For example, if everyone in the HR department need access to a Hiring Status page the administrator can assign this business role page to the department's role (HR\_ORG) rather than granting page access privileges to each department member individually. In an instant, this page gets pushed to every single user assigned to the HR\_ORG role.

If someone who is not part of the HR\_ORG role wants to see the page, like the CEO, the administrator can give this user access to the business role page too.

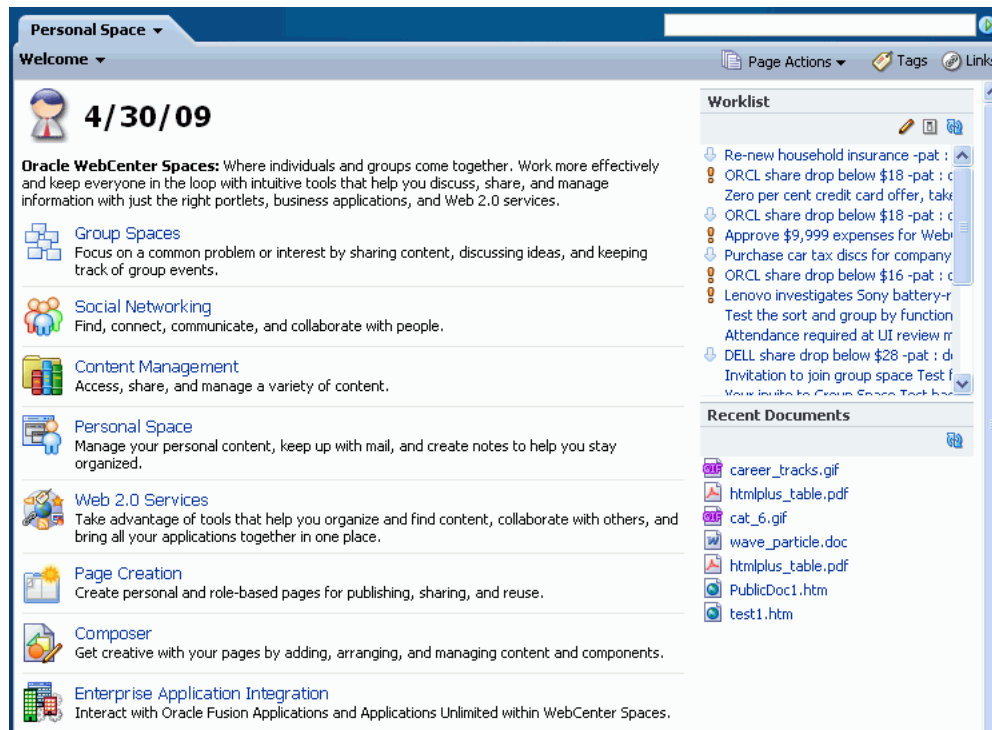
Only a WebCenter Spaces administrator can create a business role page. See [Section 20.1.2, "Creating a Business Role Page"](#). From the WebCenter Administration page, administrators can view and edit business role pages, set up page defaults, copy pages, delete pages, and manage page security.

Other users can edit, copy and delete business role pages, and change page permissions, but only if a WebCenter Spaces administrator grants them the privilege to do so. See [Section 20.1.3, "Specifying the Target Audience for Business Role Pages"](#).

### Default Welcome Page

Out-of-the-box, WebCenter Spaces provides a business role page named *Welcome* (Figure 20–1). By default, this page appears as the first page in everyone's personal space. You can edit the content of this page, change its position, hide the page from everyone, or grant custom permissions, as described in this chapter, but you cannot delete this page.

**Figure 20–1 Welcome Page - Out-of-the-box Business Role Page**



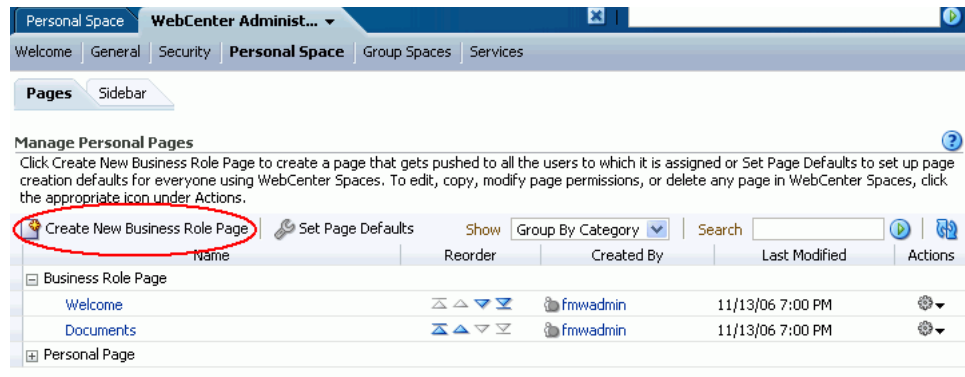
## 20.1.2 Creating a Business Role Page

To create a new business role page and push it out to a targeted audience:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Personal Space** tab.
4. Click the **Pages** tab.

All WebCenter Spaces pages are listed here, including existing business role pages (Figure 20–2).



**Figure 20–2 Viewing Business Role Pages**

5. Click **Create New Business Role Page**.
6. Enter a name for the page (**Page Name**), and then choose a **Scheme, Background Color, and Style**.

The defaults that you see on this dialog box are the same as any defaults you set for personal pages. See also, [Section 20.2.2, "Setting Up a Default Look and Feel for Personal Pages"](#).

For information about these options, see "Creating, Editing, and Deleting Pages" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

7. Click **Create**.

An empty page opens with your chosen look and feel.

You can add content to the page later on (see "Working with Page Content" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*), first lets set access permissions for the business role page.

Administrators can configure page permissions in two places—through their own Manage Pages dialog box (see "Setting and Revoking Page Access Permissions" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*) or through WebCenter Administration pages. The following steps describe the second method.

8. Next steps:
  - Add content to the page, for details, see "Working with Page Content" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.
  - Define the page audience, see [Section 20.1.3, "Specifying the Target Audience for Business Role Pages"](#).
  - Choose the page display order, see [Section 20.1.4, "Choosing a Default Display Order for Business Role Pages"](#).

Users assigned to the business role page will see this business role page in their personal space the next time they log in to WebCenter Spaces.

### 20.1.3 Specifying the Target Audience for Business Role Pages

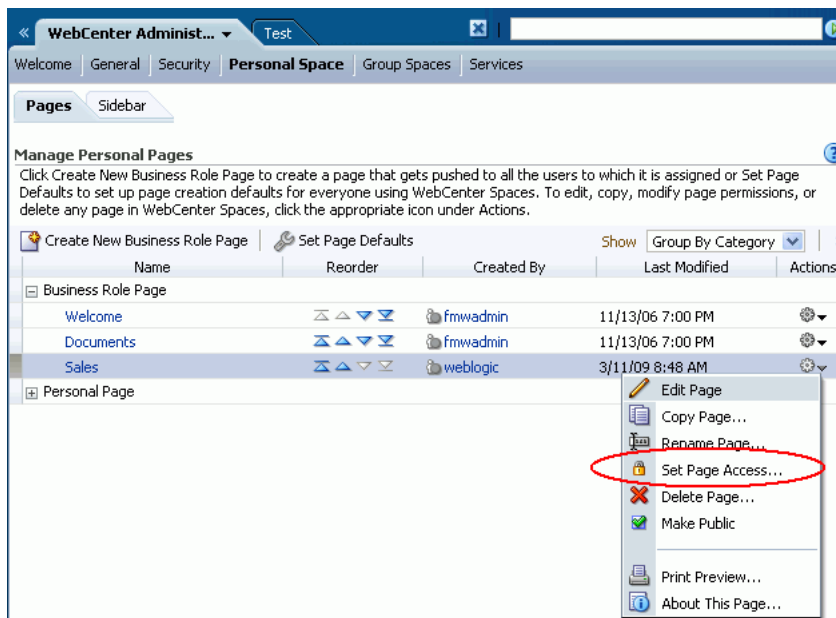
The target audience for business role pages may change from time to time. For example, you might want the whole sales team or an individual sales person to see a page originally designed for a product development team. Or maybe you want someone else to edit the page who currently does not have the *Edit Page* privilege.

Administrators can configure page permissions in two places—through WebCenter Administration pages (described below) or through their Manage Pages dialog box (see "Setting and Revoking Page Access Permissions" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*).

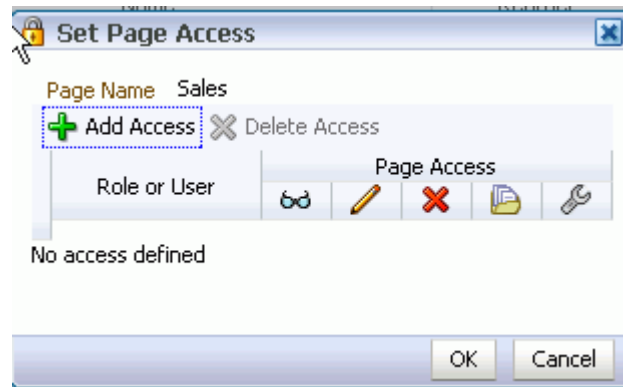
To add or change user permissions for a business role page:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Personal Space** tab.
4. Click the **Pages** tab.
5. From the **Show** drop down, choose **Group By Category**.  
The **Business Role Page** section lists every business role page in WebCenter Spaces.
6. Click the Actions icon for the page, and choose **Set Page Access** ([Figure 20–3](#)).

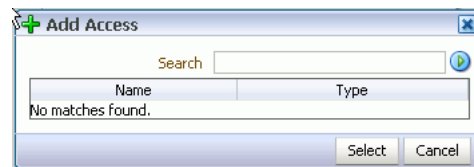
**Figure 20–3 Setting Access Permissions for a Business Role Pages**



The Set Page Access dialog box opens ([Figure 20–4](#).)

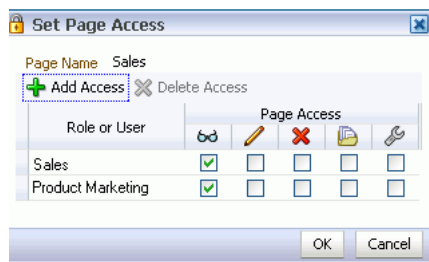
**Figure 20–4 Setting Page Access**

7. Set access permissions:
  - To grant access to additional users and roles, click **Add Access**, and then make your selection(s). Follow step 8 through 9.
  - To modify the permissions assigned to a current user or a role, select or deselect the appropriate permission check boxes. For details, see step 10.
  - To revoke access to the pages, highlight the user or the role, and then click **Delete Access**.
8. Click **Add Access**.  
The Add Access dialog box opens (Figure 20–5).

**Figure 20–5 Choosing Who Can See the Business Role Page**

9. Identify users allowed to see this business role page.  
Choose from all available users, enterprise groups, enterprise roles, and application roles. If you are not sure of their names, search your identity store:
  - a. Enter two or more characters that appear in the name you are looking for.
  - b. Click the **Search** icon.  
Users, groups, and roles matching your search criteria display in the **Add User** dialog box. The search is not case-sensitive.
  - c. Select one or more names from the list.  
To choose multiple users, multi-select all the names required. **Ctrl-Click** rows to select more than one.
  - d. Click **Select**.  
The Set Page Access dialog box displays your selections. By default, users have *view-only* permissions on the page (see Figure 20–6).

**Figure 20–6 Editing Default Page Permissions**



10. Select one or more check boxes to grant page privileges:

**View Page**—Users can view the page but cannot perform any actions on the page.

**Edit Page**—Users can edit the page. This includes adding, rearranging, and deleting content.

**Delete Page**—Users can delete the page.

**Manage Page**—Users have full access rights to the page. These users can edit the page, revise the page layout, set additional access privileges for other users, and all other page privileges.

**Personalize Page**—Users can change their personal view of the page. Such changes do not affect any other user's view of the page.

---

**Note:** To revoke a privilege, deselect the check box.

---

For more information, see [Section 19.1.3, "Understanding Application Permissions"](#).

11. Click **OK** to save your changes.

### 20.1.4 Choosing a Default Display Order for Business Role Pages

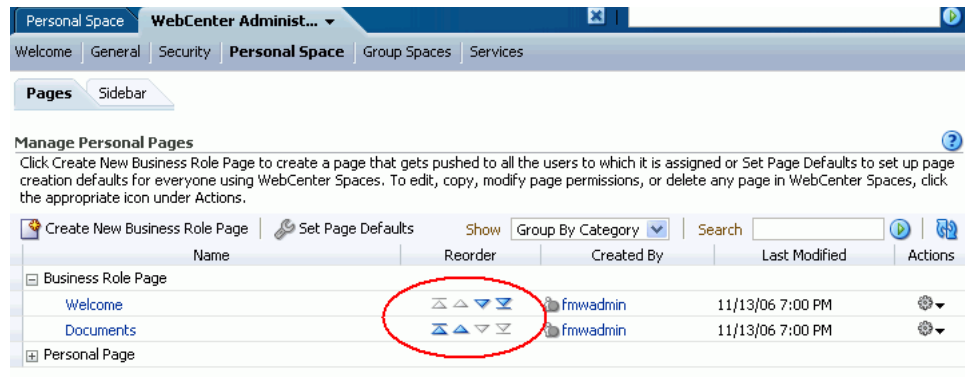
If you present business role pages in a logical order the page content is more accessible and easier for users to navigate. As administrator, you can determine the default order in which business role pages are initially presented to their intended audience.

Individual users can change the display order that you specify through their personal Page Manager if they want or hide business role pages that they do not use from their view entirely. See "Hiding, Showing, Opening, and Closing Pages" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

To change the display order of all business role pages:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Personal Space** tab.
4. Click the **Pages** tab.
5. From the **Show** drop down, choose **Group By Category**.

The **Business Role Page** section lists every business role page in WebCenter Spaces ([Figure 20–7](#)).

**Figure 20–7 Choosing a Default Display Order for Business Role Pages**

6. Click the Up and Down arrows in the **Reorder** column to change the default display order.

Alternatively, drag and drop pages into the correct position.

### 20.1.5 Editing a Business Role Page

Anyone granted the `Edit Page` permission on a business role page may edit that page. For these users, the editing process is exactly the same as for regular pages (see "Creating, Editing, and Deleting Pages" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*).

Administrators can edit any business role page from WebCenter Administration pages too.

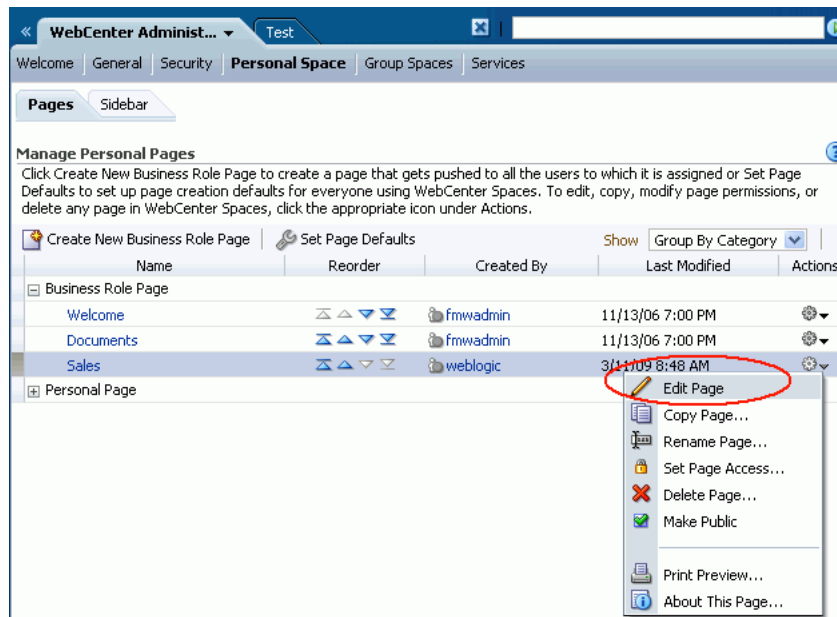
To edit a business role page through WebCenter Administration:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Personal Space** tab.
4. Click the **Pages** tab.
5. From the **Show** drop down, choose **Group By Category**.

The **Business Role Page** section lists every business role page in WebCenter Spaces.

6. Click the Actions icon for the page, and choose **Edit Page** ([Figure 20–8](#)).

**Figure 20–8 Editing Business Role Pages**



The page opens in edit mode.

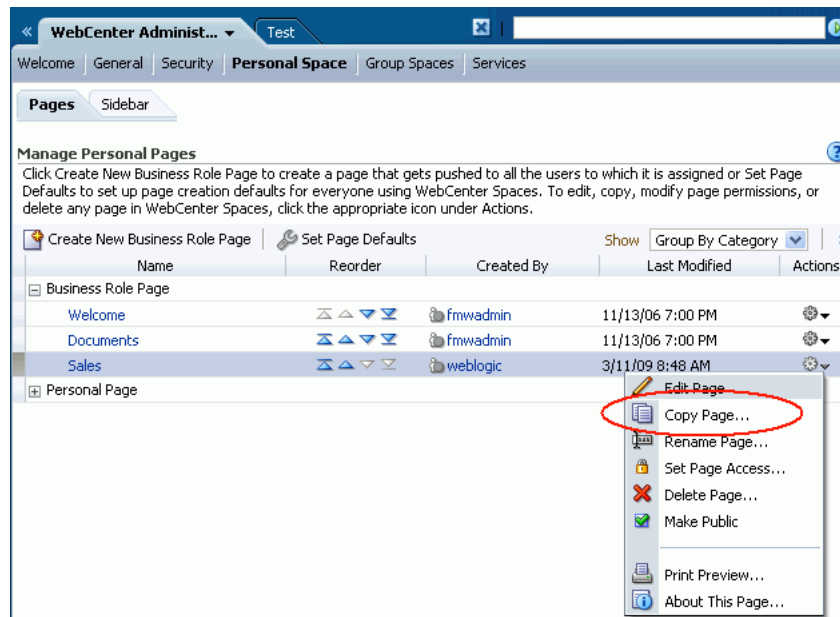
7. Update the page, and click **Save** when you are done.

### 20.1.6 Copying a Business Role Page

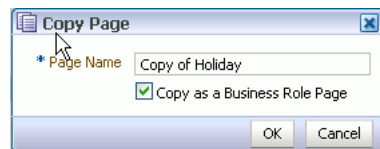
When you copy a business role page, you can save it as another business role page or as a personal page. If you create another business role page you must assign a new set of users and roles for the page as no access permissions are saved.

To copy a business role page:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Personal Space** tab.
4. Click the **Pages** tab.
5. Click the Actions icon for the page, and choose **Copy Page** ([Figure 20–9](#)).

**Figure 20–9 Copying a Business Role Page**

6. Enter a name for the new page (Figure 20–10).

**Figure 20–10 Naming the New Page**

7. Do one of the following:
  - Select **Copy as a Business Role Page** to make a copy of the page and save it as a business role page. Select this option if you intend to push the page out to a group of people with a similar job role.
  - Deselect **Copy as a Business Role Page** to keep the page copy personal.
8. Click **OK**.

The new page opens in Oracle Composer (edit mode).

### 20.1.7 Deleting a Business Role Page

Anyone granted the `Delete Page` permission on a business role page may delete it. For these users, the process is exactly the same as deleting regular pages (see "Creating, Editing, and Deleting Pages" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*).

Administrators can delete business role pages from the WebCenter Administration page too.

---

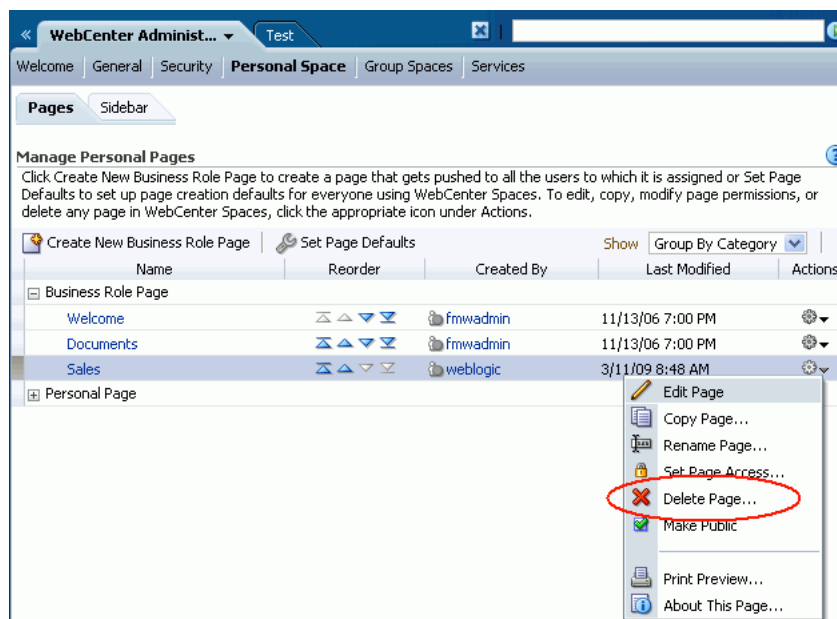
**Note:** Once a business role page is removed from WebCenter Spaces it cannot be recovered. Deleted pages are permanently removed and users previously assigned that page will no longer see it in their view.

---

To delete a business role page through WebCenter Administration:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Personal Space** tab.
4. Click the **Pages** tab.
5. Click the Actions icon for the page, and choose **Delete Page** ([Figure 20–11](#)).

**Figure 20–11 Deleting Business Role Pages**



6. Click **Delete** to confirm that you want to delete the page.

## 20.2 Managing Personal Pages

This section describes how to manage personal pages in WebCenter Spaces. It includes the following sections:

- [What You Should Know About Personal Page Management](#)
- [Setting Up a Default Look and Feel for Personal Pages](#)
- [Editing Personal Pages with Administrative Privileges](#)
- [Changing Access Permissions for a Personal Page](#)
- [Copying a Personal Page](#)
- [Deleting a Personal Page](#)

### 20.2.1 What You Should Know About Personal Page Management

In WebCenter Spaces, administrators can access everyone's personal pages from one, central place—the WebCenter Administration page. From here, administrators can view and edit personal pages, set up page defaults for everyone using WebCenter



Spaces, copy pages, and delete personal pages. Administrators can also manage page security and modify public page settings.

While individuals are primarily responsible for managing content and pages in their own personal space it is important that administrators have access too. Administrators may be required to clean up or manage personal data when owners experience difficulties with their personal pages or when owners leave the organization.

## 20.2.2 Setting Up a Default Look and Feel for Personal Pages

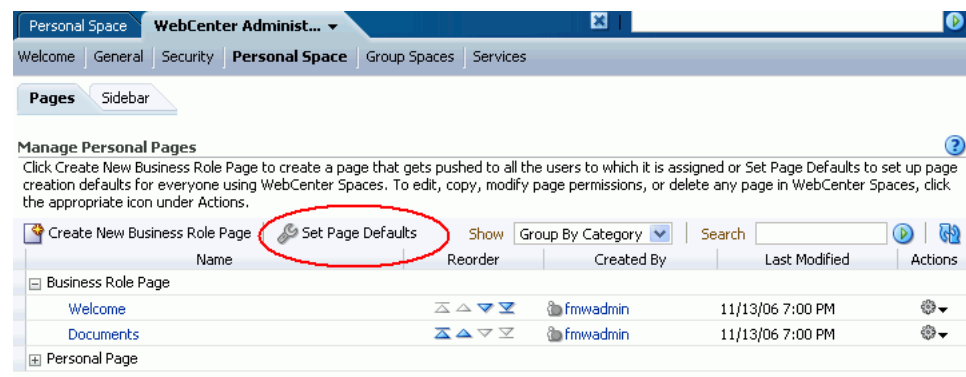
Administrators may like to set up page defaults for everyone using WebCenter Spaces. Use this feature to simplify page creation for first-time users or to steer users towards a particular page scheme and style. Individuals may override these settings through their personal Page Manager, see "Setting Page Creation Defaults for Your Personal Pages" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

Page defaults apply to personal pages and business role pages only. Defaults for pages created within the context of a group space, are controlled by the group space moderator. See "Managing Group Space Pages" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

To set up a default look and feel for personal (including business role pages):

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Personal Space** tab.
4. Click the **Pages** tab.

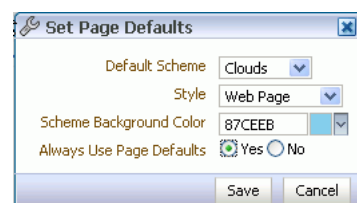
**Figure 20–12 Setting Page Defaults For Everyone**



5. Click **Set Page Defaults** ([Figure 20–12](#)).

The **Set Page Defaults** dialog box opens ([Figure 20–13](#)):

**Figure 20–13 Setting Page Defaults**



6. In the **Set Page Defaults** dialog box, select a default design scheme for all new personal pages and business role pages from the **Default Scheme** drop-down.  
A selection of background color and image schemes are provided. See also "Default Page Schemes" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.
7. Select a layout for the page structure from the **Style** drop-down.  
See also, "WebCenter Seeded Page Styles" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.
8. Specify when to apply these page defaults. For **Always Use Page Defaults**, choose from:
  - **Yes** - Personal pages and business role pages are automatically created with the defaults that you select here. If the page owner wants to use a different scheme or layout, they can edit these page properties through the Oracle Composer.
  - **No** - The scheme and style defaults you select here are presented as defaults when someone creates a personal page or an administrator creates a business role page. Page owners can override your selections before they create the page.

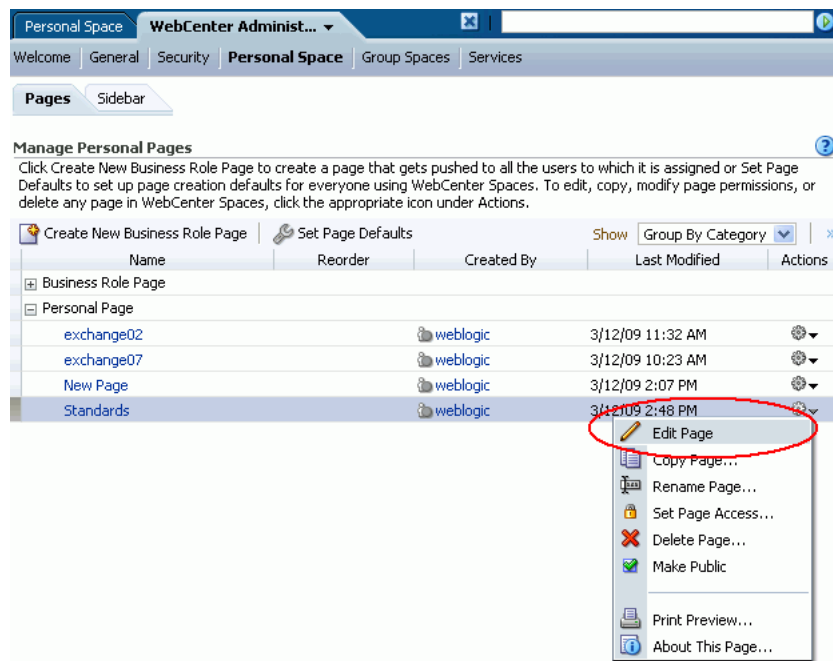
Experienced users may decide to override the defaults that you pick here by setting up page defaults of their own. See "Setting Page Creation Defaults for Your Personal Pages" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.
9. Click **Save**.

### 20.2.3 Editing Personal Pages with Administrative Privileges

Administrators are authorized to view and modify any page in a personal space, including other people's personal pages. Individuals are primarily responsible for editing content and pages in their personal space but occasionally, administrators may be required to clean up or edit personal data.

To edit a personal page as the WebCenter Spaces administrator:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Personal Space** tab
4. Click the **Pages** tab.  
The Personal Pages section lists every personal page in WebCenter Spaces.
5. Click the Actions icon for the page, and choose **Edit Page** ([Figure 20-14](#)).

**Figure 20–14 Editing Personal Pages**

The page opens in Oracle Composer. To find out more about editing page properties and page content through Oracle Composer, see:

- "Introducing Oracle Composer" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*
- "Working with Page Content" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*

6. Update the page, and click **Save** when you are done.

## 20.2.4 Changing Access Permissions for a Personal Page

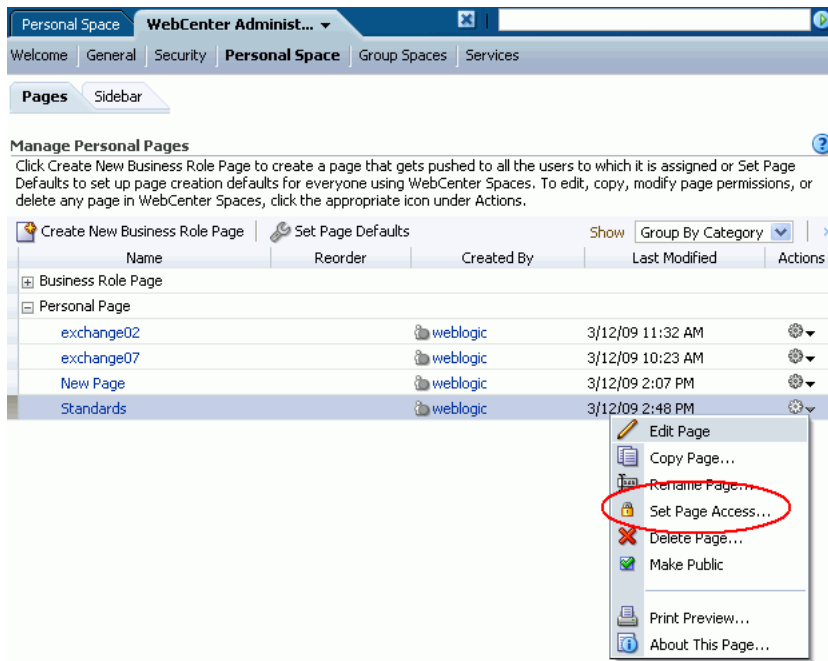
Administrators are authorized to view and manage security for any page in WebCenter Spaces and this includes personal pages. Page owners normally determine who can see their pages but occasionally, when a page owner is not available, the administrator may be required to make changes.

Administrators can configure page permissions in two places—through WebCenter Administration pages, as described here, or through their Manage Pages dialog box in the same way as regular users.

To change access permissions for a personal page as the WebCenter Spaces administrator:

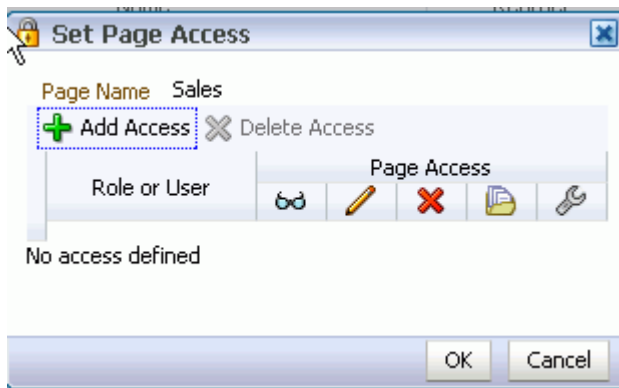
1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link.
3. Click the **Personal Space** tab.
4. Click the **Pages** tab.
5. Click the Actions icon for the page, and choose **Set Page Access** (Figure 20–15).

**Figure 20–15 Editing Page Access**



The Page Access dialog box opens (Figure 20–16).

**Figure 20–16 Setting Page Access**



6. Edit the current permissions:

- To grant access to additional users and roles, click **Add Access**, and then make your selection(s).
- To modify the permissions assigned to a current user or a role, select or deselect the appropriate permission check boxes.

**View Page**—The selected user or role can access the page for viewing, but cannot perform any actions on the page.

**Delete Page**—The selected user or role can delete the page.

**Manage Page**—The selected user or role has full access rights to the page. This means, the user can edit the page, revise the page layout, set additional access privileges for other users, and all other page privileges.

**Edit Page**—The selected user or role can edit the page. This includes adding, rearranging, and deleting content.

**Personalize**—The selected user or role can change their personal view of the page. Such changes do not affect any other user's view of the page.

---

**Note:** You can revoke privileges by taking the same steps and deselecting one or multiple privileges for a listed user or role.

---

For more information, see [Section 19.1.3, "Understanding Application Permissions"](#).

- To revoke access to the page, highlight the user or the role, and then click **Delete Access**.

## 20.2.5 Copying a Personal Page

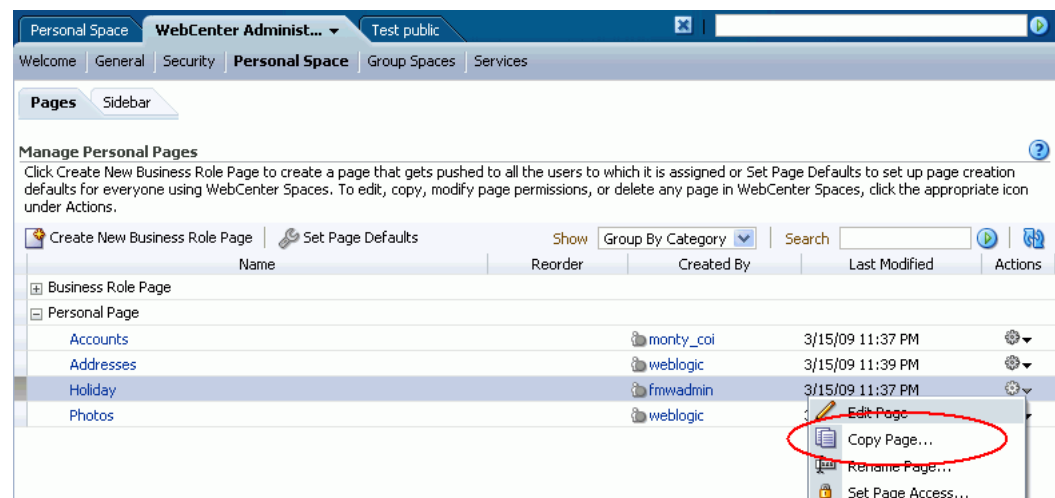
Administrators are authorized to copy any page in WebCenter Spaces, including other people's personal pages.

When you copy a personal page as an administrator, you can save it as a business role page or as a personal page owned by yourself. If you create a business role page you must assign a new set of users and roles for the page as no access permissions are saved. For more details, see [Section 20.1.1, "What You Should Know About Business Role Pages"](#).

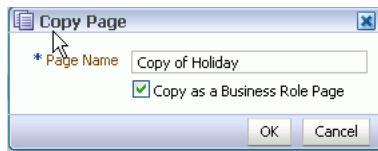
To copy a personal page as an administrator:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.y.s.
3. Click the **Personal Space** tab.
4. Click the **Pages** tab.
5. Click the Actions icon for the page, and choose **Copy Page** ([Figure 20–17](#)).

**Figure 20–17 Copying a Personal Page**



6. Enter a name for the new page ([Figure 20–18](#)).

**Figure 20–18 Naming the New Page**

7. Do one of the following:
  - Select **Copy as a Business Role Page** to make a copy of the page and save it as a business role page. Select this option if you intend to push the page out to a group of people with a similar job role.
  - Deselect **Copy as a Business Role Page** to keep the page copy personal.
8. Click **OK**.

The new page opens in Oracle Composer (edit mode).

## 20.2.6 Deleting a Personal Page

Administrators are authorized to delete any page in WebCenter Spaces, including personal pages.

Anyone granted the `Delete Page` permission on a personal page may delete it. For these users, the process is exactly the same as deleting regular pages (see "Deleting Pages" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*).

Administrators may delete personal pages from the WebCenter Administration page too.

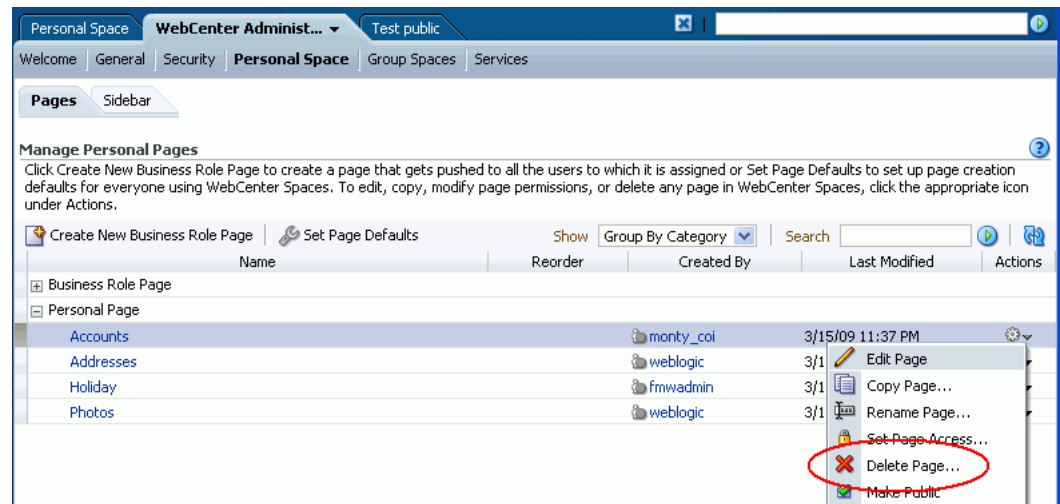
---

**Note:** Once a personal page is removed from WebCenter Spaces it cannot be recovered. Deleted pages are permanently removed.

---

To delete a personal page through WebCenter Administration:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Personal Space** tab.
4. Click the **Pages** tab.
5. Select the personal page you want to delete.
6. Click the Actions icon for the page, and choose **Delete Page** (Figure 20–19).

**Figure 20–19 Deleting Personal Pages**

7. Click **Delete** to confirm that you want to delete the page.

Deleted pages are permanently removed. You cannot recover a deleted page.

## 20.3 Setting Up the Public User Experience

By default, when unauthenticated (or public) users access the WebCenter Spaces home page they will see the public Welcome page. The Welcome page displays because it is a business role page assigned to the *anonymous-role*—it is a public page.

Other public pages provided out-of-the-box include the Login page and the Self-Registration page.

Administrators can customize the default public pages, create new public pages, or disable public access. The following sections describe how:

- [Customizing the Public Welcome Page](#)
- [Customizing the Login Page](#)
- [Customizing the Self-Registration Page](#)
- [Preventing Public Users Seeing Any Personal Page or Business Role Page](#)

### 20.3.1 Customizing the Public Welcome Page

The *public* Welcome page (Figure 20–20) displays when unauthenticated (or public) users access the WebCenter Spaces home page—the purpose of this page is to provide information and enable user login. If you decide to disable public access to all application pages the public Welcome page does not display and users are directed straight to the login page. See also, [Section 19.3.4, "Granting Permissions to the Public-User"](#).

**Figure 20–20 Public Welcome Page**

Administrators cannot use Oracle Composer to edit or change security settings for the public Welcome page provided with WebCenter Spaces.

If you want to exclude certain content or display different content on the public Welcome page you must modify the default page through JDeveloper, and deploy the customized page. Custom page deployment typically takes place *before* the WebCenter Spaces application goes live or during scheduled maintenance periods as the application's managed server must be restarted for changes to take effect.

For more information, refer to the whitepaper entitled "*Extending WebCenter Spaces*" available on the Oracle Technology Network (<http://webcenter.oracle.com>).

---



---

**Note:** The public Welcome page is different to the out-of-the-box business role page, also called *Welcome*, that everyone sees in their personal space once they are logged in to WebCenter Spaces—the default version of that page can be modified using Oracle Composer as described in Section 20.1.1, "What You Should Know About Business Role Pages". See also, Figure 20–1, "Welcome Page - Out-of-the-box Business Role Page".

---



---

### 20.3.2 Customizing the Login Page

Administrators can customize certain aspects of the default Login page through Oracle Composer. You cannot edit or delete input fields and buttons on the page but you can add new components and change the page layout if required.

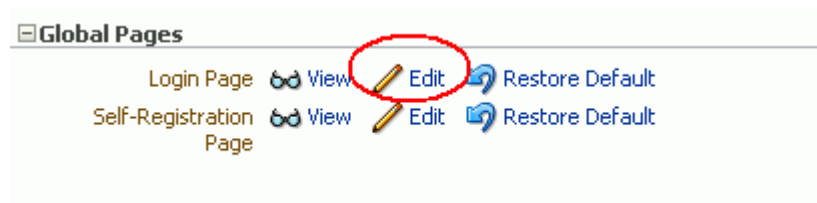
Figure 20–21 shows the Login page that is supplied out-of-the-box.



**Figure 20–21 Default Login Page**

To view and customize the Login page through WebCenter Administration:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **General** tab.
4. In the **Global Pages** section, click the **Edit** icon for the Login page ([Figure 20–22](#)).

**Figure 20–22 Edit Icon for Login Page**

Click **View** if you just want to see what the page currently looks like.

5. Edit the page in Oracle Composer ([Figure 20–23](#)).  
Add new components and change the page layout as required.

**Figure 20–23 Customizing the Login Page**



6. Click **Save** to save your changes.

You can remove all your customizations and revert back to the default Login page. To do this, click **Restore Default** (Figure 20–22).

### 20.3.3 Customizing the Self-Registration Page

The Self-Registration page allows anyone with Web access to register with WebCenter Spaces. See also, [Section 19.4, "Allowing Self-Registration"](#).

Figure 20–24 shows the default Self-Registration page that is supplied out-of-the-box. Administrators can customize certain aspects of this page through Oracle Composer. You cannot edit or delete input fields and buttons on the page but you can add new components and change the page layout if required.

For example, you might want to add some text on the page to describe your password policy.

**Figure 20–24 Default Self-Registration Page**



To view and customize the Self-Registration page through WebCenter Administration:

1. Login to WebCenter Spaces with administrative privileges.

See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).

2. Click the **Administration** link at the top of the application.
3. Click the **General** tab.
4. In the **Global Pages** section, click the **Edit** icon for the Self-Registration page (Figure 20–25).

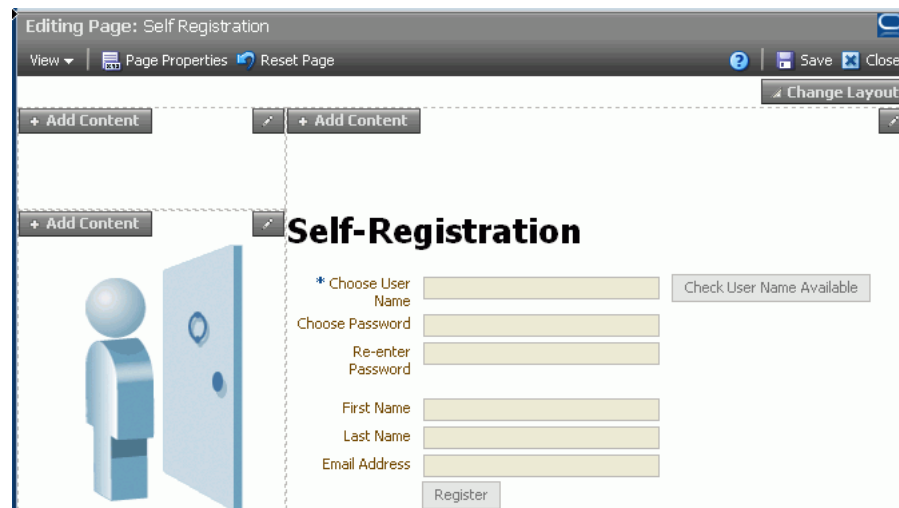
**Figure 20–25 Edit Icon for Self-Registration Page**



Click **View** if you just want to see what the page currently looks like.

5. Edit the page in Oracle Composer (Figure 20–26).  
Add new components and change the page layout as required.

**Figure 20–26 Customizing the Self-Registration Page**



6. Click **Save** to save your changes.

You can remove all your customizations and revert back to the default page. To do this, click **Restore Default** (Figure 20–25).

### 20.3.4 Preventing Public Users Seeing Any Personal Page or Business Role Page

For security reasons you may not want WebCenter Spaces users to share their personal pages with public, unauthenticated users. You can restrict public access by disabling the `Application-View` permission for all public users. For more information, see [Section 19.3.4, "Granting Permissions to the Public-User"](#).



---

# Making Applications Available in WebCenter Spaces

The Applications pane in the Sidebar provides offers WebCenter users quick access to applications they use the most. It is the WebCenter Spaces administrator's job to manage the content of the Applications pane. You control the range of applications available, the way they are presented, and how they are launched.

This section includes the following subsections:

- [What You Should Know About the Applications Pane](#)
- [Making an Application Available to WebCenter Users](#)
- [Editing Links in the Applications Pane](#)
- [Arranging the Applications List](#)
- [Locking Applications Displayed in the Applications Pane](#)
- [Removing Links from the Applications Pane](#)

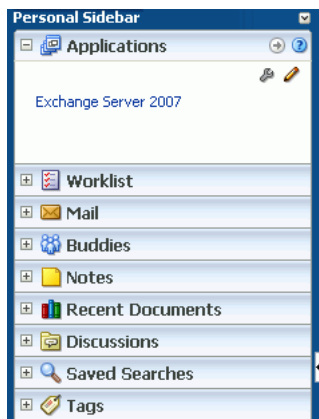
Providing they are not locked, individual WebCenter users may hide links to applications if they do not need them. See "Hiding and Showing Task Flows in the Sidebar" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

## **Audience**

The content of this chapter is intended for WebCenter Spaces administrators. Users granted the WebCenter Spaces Administrator role or a custom role that grants the Application-Manage permission).

## **21.1 What You Should Know About the Applications Pane**

WebCenter Spaces offers users centralized access to frequently-used Web applications from the Sidebar. The WebCenter Spaces administrator manages the range of applications available, the way they are presented, and how they are launched from the Applications pane ([Figure 21-1](#)).

**Figure 21–1 Sidebar - Applications Pane**

WebCenter users need not know nor care about where the information comes from, they simply click a link to launch their day-to-day applications, and if necessary, supply their user name and password information. WebCenter users may hide links that they do not use but they cannot add links of their own.

The Applications pane can launch different types of application:

- **External Applications** - Web-based, external applications that perform their own user authentication. WebCenter administrators must register external applications through the Oracle Enterprise Manager Fusion Middleware Control Console before exposing them in WebCenter Spaces. For more information, see [Section 13.2.1, "Registering External Applications Using Fusion Middleware Control"](#).
- **WebCenter Task Flows** - Built-in task flows specific to WebCenter Spaces. A range of WebCenter task flows are available out-of-the-box including Document Library Viewer, Discussions Viewer, and more. Any of these can be launched directly from the Applications pane.

For more information, see [Section 21.2, "Making an Application Available to WebCenter Users"](#).

## 21.2 Making an Application Available to WebCenter Users

The Applications pane can display links to external applications registered through Fusion Middleware Control Console as well as links to any of the built-in WebCenter task flows. When you expose an application through this pane, the application becomes available to every WebCenter user.

Some WebCenter users may not want to see all the applications offered through the Applications pane. If this is the case, individuals may personalize their view to show only those applications they must access.

To make an application available to WebCenter users:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. In the Sidebar, click the Edit icon for the Applications pane ([Figure 21–2](#)).  
If you do not have administrative privileges you will not see this icon.

**Figure 21–2 Applications Pane - Edit Icon**

When you edit the Applications pane, every WebCenter user will see your changes.

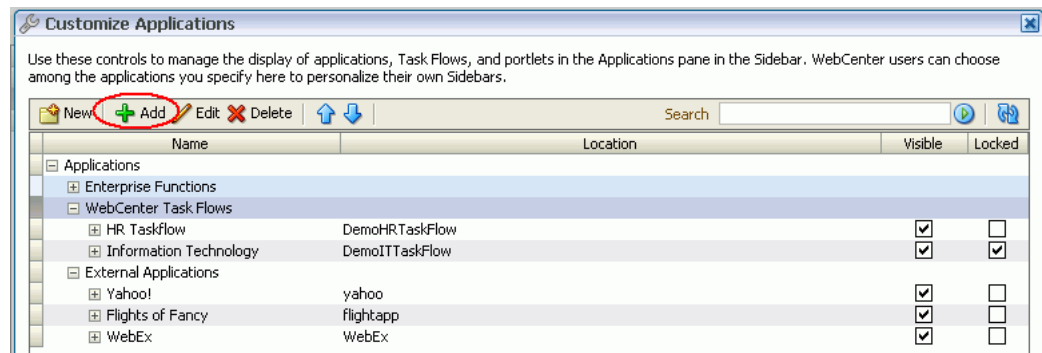
---

**Note:** For information about the Sidebar, see "Working with the WebCenter Spaces Sidebar" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

---

3. To add a link to an application, select the folder where you want the link to appear, and then click the green Add icon (Figure 21–3).

To add a new folder, click the New icon. To create a subfolder, expand the parent folder first. [Section 13.2, "Registering External Applications"](#)

**Figure 21–3 Editing the Applications Pane**

4. Navigate to the external application or task flow you require, and click its associated Add link (Figure 21–4).

- To navigate to a previously registered external application, expand the **External Applications** node, and then expand the required application.

Only registered external applications which have a *Login URL* defined appear in this list. If the application you want is not listed, ask your WebCenter administrator to register the application for you. See also [Section 13.2, "Registering External Applications"](#).

- To navigate to a task flow, expand the **WebCenter Task Flows** node. If necessary, expand one or more subfolders to access the required task flow.

If you are not sure of the exact name, enter a full or partial search term in the **Search** box, and then click **Find** to search for the application. Application names matching your search criteria are displayed.

**Figure 21–4 Choosing an Application**



An information message displays indicating whether the application link was successful.

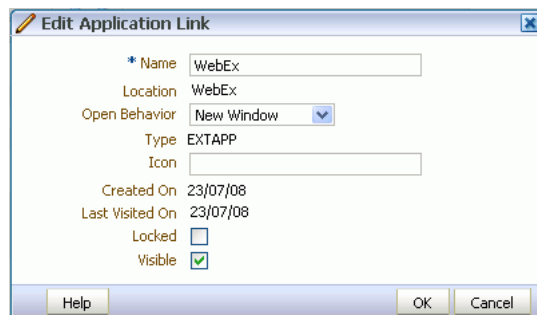
5. Click **OK** to dismiss the message box.
6. To add another application, repeat steps 4 and 5.
7. Click **OK** to return to the Edit Applications dialog box.

The selected application(s) appears within your chosen folder. From here, you can change the display name for the application link and set other display-related properties.

8. To edit link details for an application, highlight the row in the table and then click the Edit icon.

The Edit Application Link dialog box opens ([Figure 21–5](#)).

**Figure 21–5 Editing Application Links**



9. Edit the link display properties, as required.  
For details, see [Table 21–1, " Application Link Properties"](#):



**Table 21–1 Application Link Properties**

| Property        | Description  |
|-----------------|--|
| Name            | Enter the link text that WebCenter users will click to launch the application.   |
| Location        | (Read-only) Displays the internal name for the application or task flow.   |
| Open Behavior   | Choose how the application displays when users click the link: <ul style="list-style-type: none"> <li>■ <b>WebCenter Tab</b> - Application displays as a tab in WebCenter Spaces, and the application displays there. The current WebCenter Spaces context is maintained.</li> <li>■ <b>New Window</b> - Application opens in a new browser window. The current WebCenter Spaces context is maintained. This is the default selection.</li> <li>■ <b>Current Window</b> - Application opens in the current browser window (in place of WebCenter Spaces).</li> </ul> |
| Type            | (Read-only) Displays the link type: EXTAPP - External application or TASKFLOW - WebCenter task flow  |
| Icon            | Associate an icon with the application. Enter a full qualified URL or a relative URL that specifies the location of a valid icon.<br>The icon displays alongside the link in the Sidebar. For best results, choose an icon that is 16 x 16 pixels.   |
| Created On      | Shows when the link was created.   |
| Last Visited On | Shows the last time a user clicked the link.<br>If a link is not used very often or at all, you might consider removing it from the Applications pane.   |
| Locked          | Indicate whether WebCenter users are allowed to show/hide the link.<br>Select <b>Locked</b> to prevent users from showing/hiding the link. Deselect <b>Locked</b> to let the user decide whether the link displays in their personal view. Individuals users can show or hide the link depending of whether they need access to the application from the Sidebar.  |
| Visible         | Indicate whether WebCenter users see a link to this application in the Applications pane.<br>Select <b>Visible</b> to show the link. Deselect <b>Visible</b> to hide the link.   |

10. Click **OK** to save.

11. Click **Close** to dismiss the Edit Application Link dialog box.

New or updated links appear in the Applications pane. Click the link to test that it works correctly.

## 21.3 Editing Links in the Applications Pane

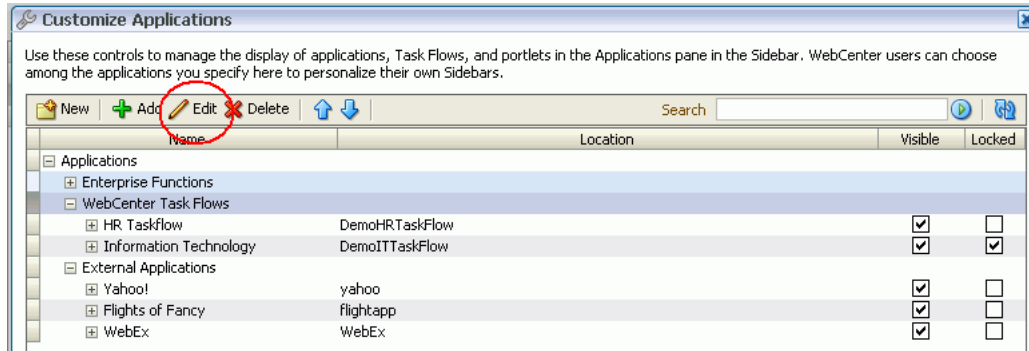
To edit a link displayed in the Applications pane:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. In the Sidebar, click the Edit icon for the Applications pane.

**Note:** When you edit the Applications pane, every WebCenter user sees your changes.

3. Select an application link by highlighting the row in the table.
4. Click the Edit icon (Figure 21–6).

**Figure 21–6** Editing Application Links

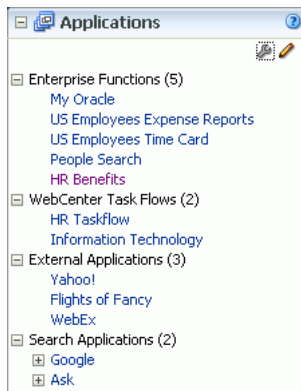


5. Edit the link properties, as required. For details, see [Table 21–1, "Application Link Properties"](#).
6. Click OK to save.
7. Click Close to dismiss the Edit Applications dialog box.

## 21.4 Arranging the Applications List

As WebCenter Spaces administrator, you choose the display order of links in the Applications pane. You can also organize your application links into a hierarchy by creating sub folders. These sub folders, which can represent topic areas, can be nested into other sub folders (Figure 21–7).

**Figure 21–7** Arranging the Applications List



1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. In the Sidebar, click the Edit icon for the Applications pane.

**Note:** When you edit the Applications pane, every WebCenter user sees your changes.

3. Reorganize your applications. For example:
  - **Rearrange the display order.** Select an application or a folder, and then click the Move Up and Move Down icons until it appears in the correct place. When you move a folder, everything under the folder moves with it.  
Alternatively, drag and drop an application to the correct position.
  - **Create a new folder or sub folder.** Select a parent folder (if required), click the New Folder icon, enter a suitable **Name**, and then click **Create**.
  - **Rename a folder.** Click the **Display Name** and edit the folder name in place.
4. Click **Close** to save.

## 21.5 Locking Applications Displayed in the Applications Pane

WebCenter Spaces administrators can lock links displayed in the Applications pane. When you lock a link, WebCenter users are not allowed to show/hide the link.

Unlock links to let the user decide whether the link displays in their personal view. Individuals users can show or hide the link depending of whether they need access to the application from the Sidebar.

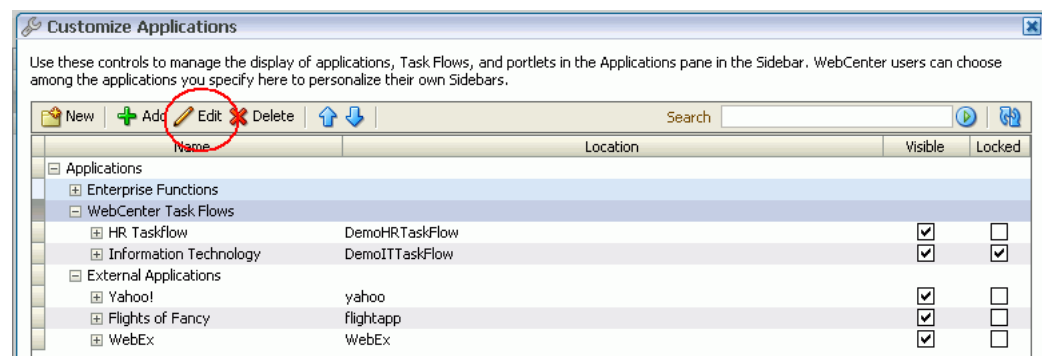
To lock an application link:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. In the Sidebar, click the Edit icon for the Applications pane.

**Note:** When you edit the Applications pane, every WebCenter user will see your changes.

3. Select the required application by highlighting the row in the table.
4. Click the Edit icon ([Figure 21-8](#)).

**Figure 21-8 Editing Application Links**



5. To lock the application, select **Locked**.

6. Click **OK** to save.
7. Click **Close** to dismiss the Edit Applications dialog box.

## 21.6 Removing Links from the Applications Pane

When application links are no longer required, WebCenter Spaces administrators can remove them from the Applications pane.

Removing links is permanent. If a link might be useful in the future, consider hiding the link instead (by deselecting the **Visible** property). For details, see [Section 21.3, "Editing Links in the Applications Pane"](#).

To permanently remove an application link:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. In the Sidebar, click the Edit icon for the Applications pane.

---

---

**Note:** When you edit the Applications pane, every WebCenter user will see your changes.

---

---

3. Select the required application (or application folder) by highlighting the row in the table.
4. To remove the application link, click the Delete icon.  
When you delete a folder, you delete the folder and all the applications displayed in the folder.
5. Click **Delete** to confirm.
6. Click **Close** to dismiss the Edit Applications dialog box.

---

## Managing Group Spaces in WebCenter Spaces

This chapter describes how a WebCenter Spaces administrator with `Group Space-Manage` or `Group Space Template-Manage` permissions can manage everyone's group spaces and group space templates in WebCenter Spaces. It includes the following sections:

- [What You Should Know About Group Space Management](#)
- [Viewing Group Space Information](#)
- [Changing the Status of a Group Space](#)
- [Enabling and Disabling Services](#)
- [Managing Group Space Templates](#)
- [Publishing and Unpublishing Group Space Templates](#)

For more information about exporting and importing group space information, see [Chapter 23, "Exporting and Importing Group Spaces"](#).

### Audience

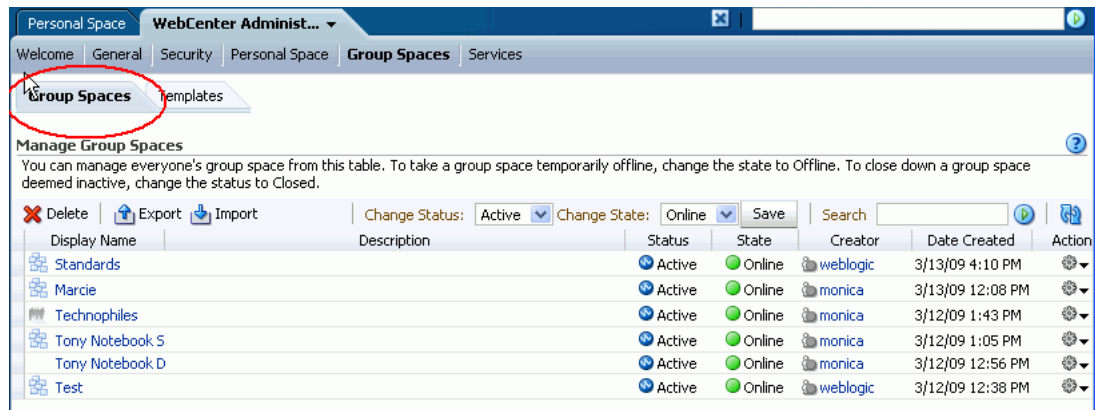
The content of this chapter is intended for WebCenter Spaces administrators. Users granted the `WebCenter Spaces Administrator` role or a custom role that grants the `Application-Manage` permission).

## 22.1 What You Should Know About Group Space Management

WebCenter Spaces administrators with `Group Space-Manage` or `Group Space Template-Manage` permissions can manage any group space or group space template from WebCenter Administration pages ([Figure 22-1](#)). From here, you can take any group space temporarily offline and close down any group spaces deemed inactive. Administrators can rename and edit any group space, as well as delete group spaces when they are no longer required.

Group space moderators do not have access to this page. While group space moderators may perform *some* of these tasks for group spaces that they own through group space administration, the WebCenter Spaces administrator can manage all of them.

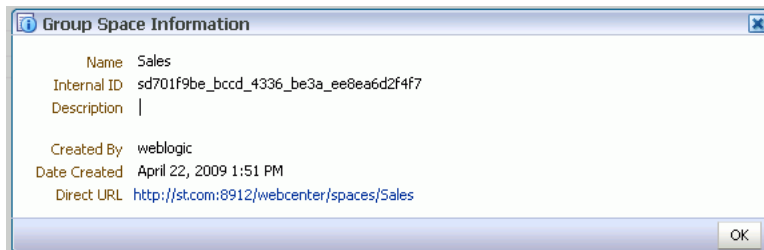
The Group Spaces administration page offers import and export services too. To find out more, see [Chapter 23, "Exporting and Importing Group Spaces"](#).

**Figure 22–1 WebCenter Administration - Group Spaces**

## 22.2 Viewing Group Space Information

WebCenter Spaces administrators can view and manage any group space through WebCenter Administration pages. From here, you can quickly see whether group spaces are active, online, offline, who created the group space (the group space moderator), and on which date group spaces were created.

The Actions menu offers additional options for editing, renaming, and deleting group spaces, and if you select *About Group Space* you can access useful information such as the group's space direct URL and internal ID (Figure 22–2).

**Figure 22–2 About Group Space**

By default, group spaces are listed alphabetically. To view the information differently, by *Create Date* for example, click the sort icon for the column. Sort icons appear when you hover over the mouse over the column header.

To display the group space administration page:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Group Spaces** tab.
4. Click the **Group Spaces** subtab.

## 22.3 Changing the Status of a Group Space

WebCenter Spaces administrators can change the status of any group space. The following sections tell you how:

- [Taking Any Group Space Offline](#)
- [Bringing Any Group Space Back Online](#)
- [Closing Any Group Space](#)
- [Reactivating Any Group Space](#)
- [Deleting a Group Space](#)

### 22.3.1 Taking Any Group Space Offline

When a group space is offline, members of the group space are unable to access the group space. If members try to access the group space, they will see the *Group Space Unavailable* page. See also "Customizing the Group Space Unavailable Page" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

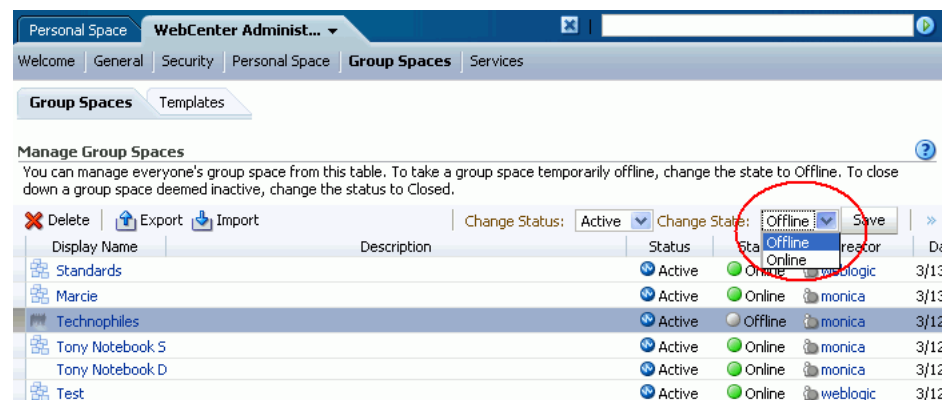
Administrators and group space members with Group Space-Manage permissions may access a group space that is offline. So if, for example, an administrator notices inappropriate content they can take a group space offline, fix the content, and bring it back online later.

To permanently close down a group space that is not being used any more, see [Section 22.3.3, "Closing Any Group Space"](#).

To take a group space offline:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Group Spaces** tab.
4. Click the **Group Spaces** subtab.
5. Select the group space you require by highlighting the row in the table.
6. From the **Change State** drop down, select **Offline** ([Figure 22–3](#)).

**Figure 22–3 Taking a Group Space Offline**



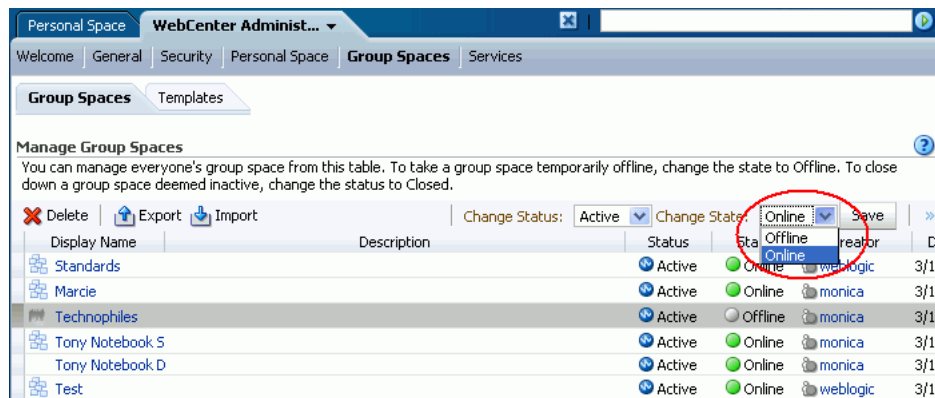
7. Click **Save**.

### 22.3.2 Bringing Any Group Space Back Online

To bring any group space back online:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Group Spaces** tab.
4. Click the **Group Spaces** subtab.
5. Select the required group space by highlighting the row in the table.
6. From the **Change State** drop down list, select **Online** ([Figure 22–4](#)).

**Figure 22–4 Bringing a Group Space Online**



7. Click **Save**.

### 22.3.3 Closing Any Group Space

A WebCenter Spaces administrator can close any group space that is no longer being used. When you close a group space the content is archived. The group space is removed from everyone's Group Space menu to avoid clutter but its content remains accessible and searchable to those who may want to reference it.

Current members may still access the group space through My Group Spaces. See "Viewing Available Group Spaces" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

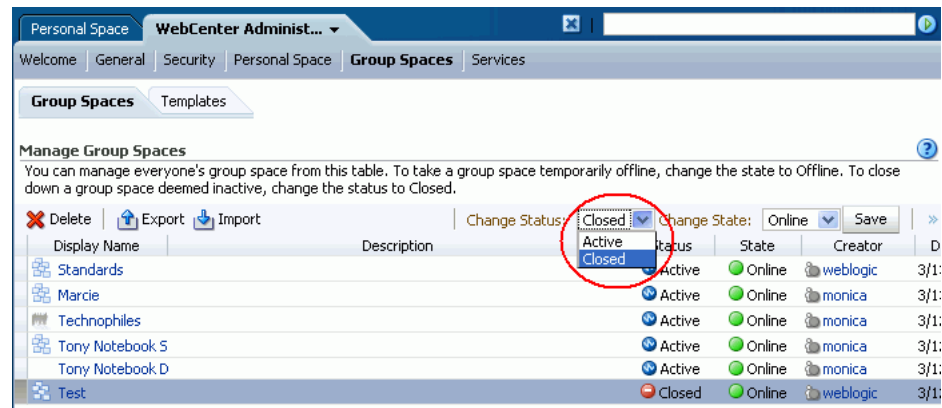
If you want to close down a group space temporarily, take the group space offline instead. See [Section 22.3.1, "Taking Any Group Space Offline"](#).

To close a group space:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Group Spaces** tab.
4. Click the **Group Spaces** subtab.
5. Select the required group space by highlighting the row in the table.
6. From the **Change Status** drop down, select **Closed** ([Figure 22–5](#)).



Figure 22–5 Closing a Group Space



7. Click **Save**.

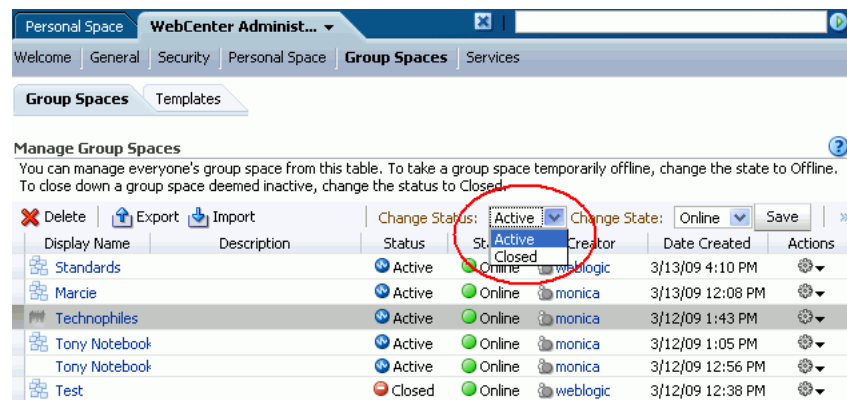
### 22.3.4 Reactivating Any Group Space

WebCenter Spaces administrator and group space moderators may close a group space if it is no longer being used. If you want to reopen a group space, you can do so.

To reactivate a group space:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Group Spaces** tab.
4. Click the **Group Spaces** subtab.
5. Select the required group space by highlighting the row in the table.
6. From the **Change Status** drop down, select **Active** (Figure 22–6).

Figure 22–6 Activating a Group Space



7. Click **Save**.

## 22.3.5 Deleting a Group Space

WebCenter Spaces administrators with the `Group Space-Manage` permission can delete any group space. Once a group space is removed from WebCenter Spaces it cannot be recovered. Group spaces are permanently removed and current members will no longer see the group space in their view.

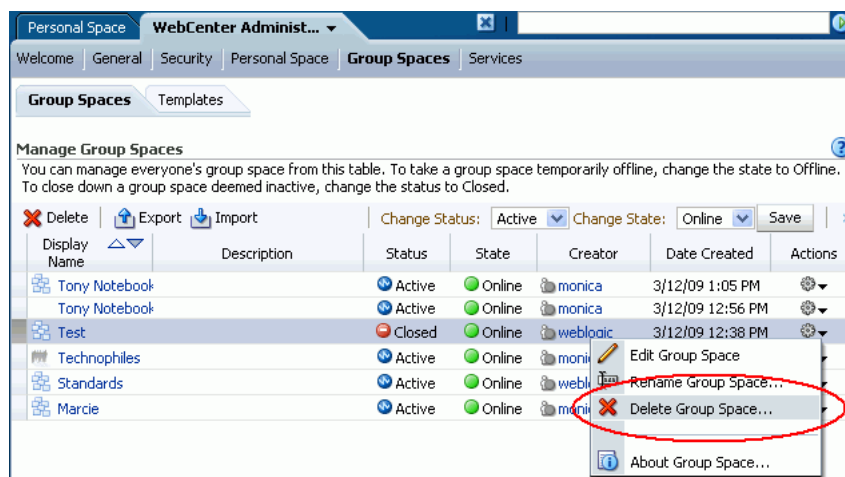
Most group space data is deleted too; the exceptions are group space discussions, announcements, wikis, and blogs which remain on the associated back-end servers.

You cannot delete a group space while the moderator is editing group space settings but there are no other restrictions.

To delete a group space that is no longer required:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Group Spaces** tab.
4. Click the **Group Spaces** subtab.
5. Select the required group space by highlighting the row in the table.  
**Ctrl-Click** rows to select more than one.
6. Click the Actions icon for the page, and choose **Delete** ([Figure 22–7](#)).

**Figure 22–7 Deleting a Group Space**



7. Click **Delete** to confirm that you want to delete the group space(s).

If the delete process fails for any reason, the group space is not removed from the administrator's Group Space tab; this sometimes happens when a back-end server cannot be contacted. If administrator's click Delete again from here, the group space will be removed.

## 22.4 Enabling and Disabling Services

WebCenter Spaces services, such as Discussions and Mail, are configured by your Fusion Middleware Administrator through Fusion Middleware Control or using the WLST command-line tool. New services automatically become available in WebCenter Spaces when the application starts up—no additional configuration is required inside

WebCenter Spaces. Likewise, there is no facility to disable services for the entire application as the Fusion Middleware Administrator takes care of this through Fusion Middleware Control. See also, [Section 2, "Getting WebCenter Spaces Up and Running"](#).

You can enable and disable services for individual group spaces inside the WebCenter Spaces application: Announcements, Discussions, Documents, Group Space Events, Instant Messaging and Presence, Lists and Mail. In most cases, the group space moderator will manage service requirements for their own group space but WebCenter Spaces administrators can also perform this task if required to do so. For details, see "Enabling and Disabling Services Available to a Group Space" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

## 22.5 Managing Group Space Templates

WebCenter Spaces administrators with the Group Space Template-Manage permission can review and delete any group space template. The following sections tell you how:

- [What You Should Know About Managing Group Space Templates](#)
- [Viewing Group Space Templates](#)
- [Deleting a Group Space Template](#)

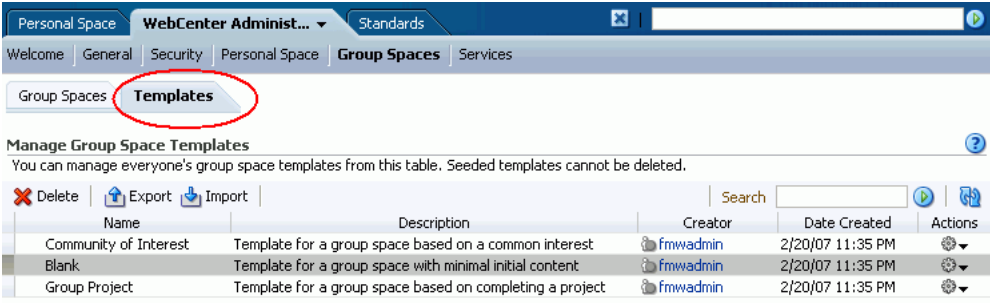
### 22.5.1 What You Should Know About Managing Group Space Templates

WebCenter administrators with the Group Space Template-Manage permission can manage *every* group space template from the Group Space Template administration page ([Figure 22–8](#)). You can see which group space templates are currently available, and delete group space templates when they are no longer required. You can also publish templates—making them available to everyone—or restrict them to private use only.

It is important to keep the template list up to date and valid. Anyone who creates a group space will see public templates as well as their own private templates.

The Group Space Templates administration page provides import and export services too. To find out more, see [Chapter 23, "Exporting and Importing Group Spaces"](#).

**Figure 22–8 WebCenter Administration - Templates Page**



| Name                  | Description  | Creator  | Date Created     | Actions |
|-----------------------|--|----------|------------------|---------|
| Community of Interest | Template for a group space based on a common interest    | fmwadmin | 2/20/07 11:35 PM | ⚙️      |
| Blank                 | Template for a group space with minimal initial content  | fmwadmin | 2/20/07 11:35 PM | ⚙️      |
| Group Project         | Template for a group space based on completing a project | fmwadmin | 2/20/07 11:35 PM | ⚙️      |

### 22.5.2 Viewing Group Space Templates

WebCenter Spaces administrators with the Group Space Template-Manage permission can view and manage any group space through WebCenter Administration pages. From here, you can quickly see who created each group space template (the group space moderator), and the date on which it was created. The Actions menu

offers additional options for deleting group space templates, and you can publish and unpublish templates from here too.

By default, group space templates are listed alphabetically. To view the information differently, by *Create Date* for example, click the sort icon for the column. Sort icons appear when you hover over the mouse over the column header.

To see a list of every group space template in WebCenter Spaces, together with their description, creator, and other useful information:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Group Spaces** tab.
4. Click the **Templates** tab.

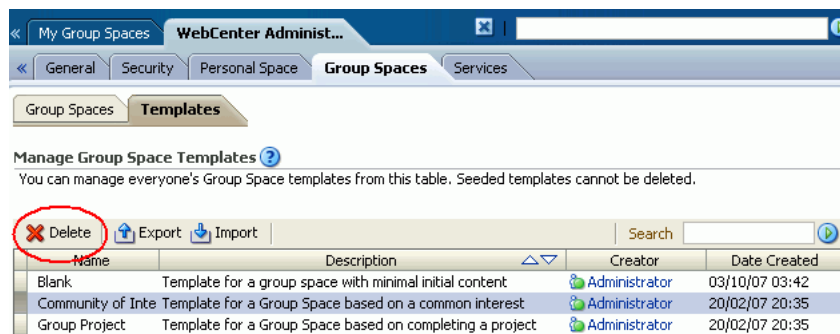
### 22.5.3 Deleting a Group Space Template

WebCenter Spaces administrators with the `Group Space Template-Manage` permission can delete any group space template except the standard, out-of-the-box templates: Blank, Community of Interest, Group Project.

To delete a group space template that is no longer required:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Group Spaces** tab.
4. Click the **Templates** tab.
5. Select the required template by highlighting the row in the table.  
**Ctrl-Click** rows to select more than one.
6. Click the **Delete** icon ([Figure 22–9](#)) or choose **Delete Group Space Template** from the Actions menu.

**Figure 22–9 Deleting a Group Space Template**



7. Click **Yes** to confirm that you want to delete the selected template(s).

## 22.6 Publishing and Unpublishing Group Space Templates

Several group space templates are provided out-of-the-box: Group Project, Community of Interest, and Blank. In addition to these, users with the `Group Space-Create` permission can create customized templates from group spaces and share them with other users.

While WebCenter Spaces can accommodate any number of templates, a limited number of templates is sometimes more effective. Administrators with the `Group Space Template-Manage` permission can maintain the template list through WebCenter Administration.

To publish or unpublish a group space template:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Group Spaces** tab.
4. Click the **Templates** tab.
5. From the Actions menu, choose:
  - **Publish Group Space Template** - to share the template with everyone.
  - **Make Group Space Template Private** - to remove the template from the group space template list. The template owner can use the template but nobody else will see it.
6. Confirm your selection.



---

## Exporting and Importing Group Spaces

Oracle WebCenter provides a set of export and import utilities that enable you to back up or move group space information between WebCenter applications, and stage or production environments. This chapter describes how to export and import group spaces and group space templates through WebCenter Spaces administration page. It includes the following sections:

- [Exporting Group Spaces](#)
- [Importing Group Spaces](#)
- [Exporting Group Space Templates](#)
- [Importing Group Space Templates](#)

Fusion Middleware Administrators can also export/import group spaces and group space templates using WLST commands. To find out more about these WLST commands, how to migrate the back-end data associated with group spaces, as well as how to export an entire WebCenter Spaces application, see [Section 16.1, "Exporting and Importing WebCenter Spaces for Data Migration"](#).

### Audience

The content of this chapter is intended for WebCenter Spaces administrators. Users granted the WebCenter Spaces Administrator role or a custom role that grants the Application-Manage permission).

## 23.1 Exporting Group Spaces

WebCenter Spaces administrators can export group spaces and import them into other WebCenter Spaces applications. Group spaces must be taken offline, even if only temporarily, to prevent data conflicts during the export process. See, [Section 22.3.1, "Taking Any Group Space Offline"](#).

Group space information is exported into a single export archive (.ear file). The EAR file contains a metadata archive (.mar file) and, optionally, a single XML file containing group space security policy information. You can save export archives to your local file system or to a remote server file system.

For more information about what is exported, read [Section 16.1.1, "Understanding WebCenter Spaces Export and Import"](#)

The export process does not include data associated with external services such as Mail, Discussions, Announcements, Wikis, Blogs, Instant Messaging and Presence, and Documents, as all this data is stored on external servers. To learn how to move data associated with these services, refer to documentation for that product. See also, [Section 16.1.7, "Migrating Back-end Components for Individual Group Spaces"](#).

---



---

**Note:** No icons, skins, images, or personalizations are exported. Personalizations are changes that individuals make to their personal view of a group space. See also, "Personalizing Your Page View" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.

---



---

WebCenter Spaces administrators can export group spaces through WebCenter Spaces Administration as described here. Fusion Middleware administrators can also export group spaces using WLST commands. For details, see [Section 16.1.9.2, "Importing Group Spaces Using WLST"](#).

You can also export group space templates but this is a separate process. You cannot export group spaces and group space templates into a single archive. For details, see [Section 23.3, "Exporting Group Space Templates"](#).

To export one or more group spaces using WebCenter Spaces:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Group Spaces** tab.
4. Click the **Group Spaces** subtab.
5. Select the group space required by highlighting the row in the table.

To select multiple group spaces, **Ctrl-click** or **Shft-click** multiple rows.

Ensure that all the group spaces you select are *offline*. Group spaces must be taken offline, even if only temporarily, to prevent data conflicts during the export process. Unsaved changes are not exported. See also [Section 22.3.1, "Taking Any Group Space Offline"](#).

---



---

**Note:** Members with the `Group Space-Manage` permission should avoid editing group spaces that are taken offline during the export process.

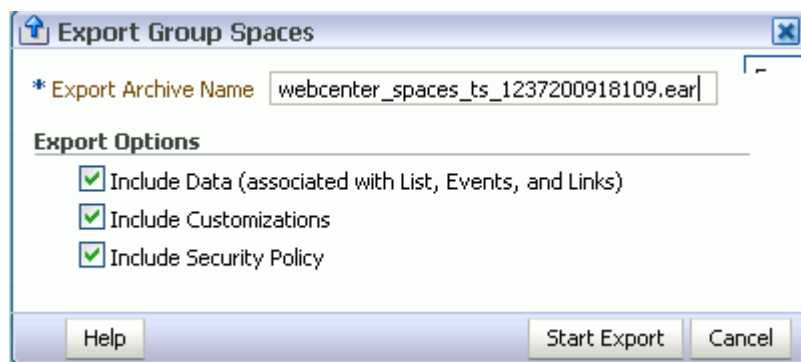
---



---

6. Click **Export** in the toolbar.  
The Export Group Spaces dialog box opens ([Figure 23–1](#)).

**Figure 23–1 Exporting Group Spaces**



7. Change the **Export Archive Name** or accept the default name.



To ensure uniqueness, the default .ear filename contains a timestamp:  
 webcenter\_spaces\_ts\_<timestamp>.ear

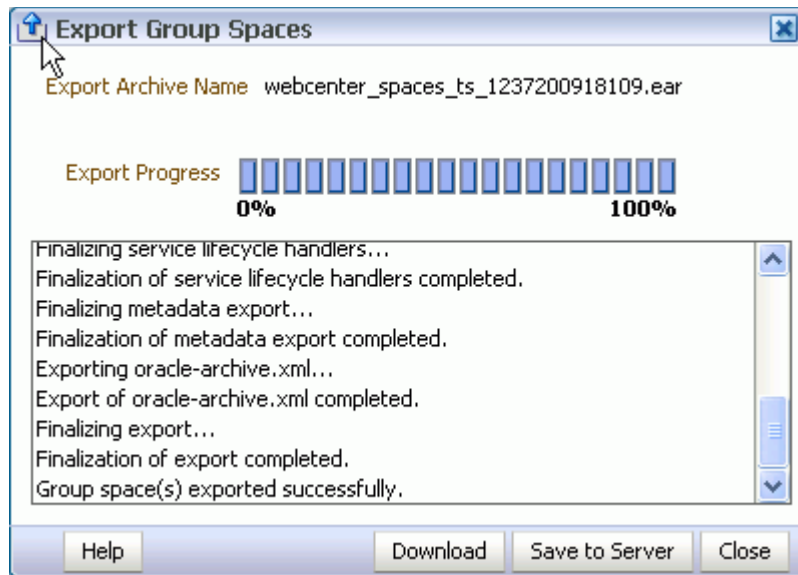
8. Set export options as required. For details, see [Table 23–1](#):

**Table 23–1 Group Space Export Options**

| Field                   | Description   |
|-------------------------|---|
| Include Data            | <p>Select to export data stored in the WebCenter repository for Lists, Events, and Links. For example, list items, group space events, and links/associations between objects in the group space.</p> <p>If the group spaces selected for export contain a large amount of data, consider using the database export utilities to move the WebCenter schema data instead. For example</p> <pre>DB_OH/bin/expdp \ "sys/password@dbhost as sysdba\" schemas=RCUPREFIX_WEBCENTER directory=data_pump_dir dumpfile=WC.dmp</pre> <p>Deselect this option if you do not want to export any data associated with lists, events, and links. For example, when moving a group space from a test environment to a stage or production environment where test data is not required.</p>   |
| Include Customizations  | <p>Select to export group space customizations. For information about which customizations are optional on export, see <a href="#">Table 16–1</a> and <a href="#">Table 16–2</a>.</p> <p>If you deselect this option, WebCenter Spaces is exported without these group space customizations.</p> <p>Portlet and page customizations are always exported. See also <a href="#">Figure 16–1</a>, "Information Exported with WebCenter Spaces".</p>  |
| Include Security Policy | <p>Select to migrate security information with the group space.</p> <p>When selected, an XML file is generated (<code>policy-store.xml</code>) containing the following security related information:</p> <ul style="list-style-type: none"> <li>■ Group space roles (and permissions assigned to each role).</li> <li>■ Group space members (and member role assignments).</li> </ul> <p>Deselect this option if you do not want to export group space security information. This option is useful when exporting group spaces between a stage and production environments, where:</p> <ul style="list-style-type: none"> <li>■ Members used during testing are not required in the production environment.</li> <li>■ The group space already exists on the production instance and you do not want to overwrite the security information.</li> </ul> <p><b>Note:</b> When exporting a brand new group space, always select (check) this option as you cannot import a new group space without a security policy.</p> |

9. Click **Start Export**.

Progress information is displayed during the export process ([Figure 23–2](#)).

**Figure 23–2 Exporting Group Spaces In Progress**

10. When the export process is complete, specify a location for the export archive (.ear). Select one of:
  - **Download** - Saves the export EAR file to your local file system.  
Your Browser downloads and save the archive locally. The actual download location depends on your Browser set up.
  - **Save to Server** - Saves the export .ear file to a server location. For example, /tmp. Ensure that there are write permissions on the sever directory that you specify.  
After clicking **Save to Server**, enter the **Server Location** and then click **Save**.
11. Click **Close** to dismiss the Export Group Spaces window.  
The export archive (.ear) is saved to the specified location.

## 23.2 Importing Group Spaces

WebCenter Spaces administrators can import a group space archive (.ear) into another WebCenter Spaces application.

On import, *all* group spaces included in the archive are created or re-created on the target application. Existing group spaces are deleted then replaced, and new group spaces are created.

Group spaces must have a security policy. When you import a brand new group space you must ensure that the group space's security policy is included in the export archive. Existing group spaces already have a security policy in place so in this case, it's up to you whether to overwrite the security information on import or maintain the existing security policy.

If data migration is important, group space documents, discussions, and wikis and blogs can be migrated for individual group spaces. For details, see [Section 16.1.7, "Migrating Back-end Components for Individual Group Spaces"](#).

WebCenter Spaces administrators can export group spaces through WebCenter Spaces Administration as described here. Fusion Middleware administrators can also export

group spaces using WLST commands. For details, see [Section 16.1.9.2, "Importing Group Spaces Using WLST"](#)

WebCenter Spaces does not support concurrent import operations. To avoid potential conflicts, import and export operations are disallowed while an import is in progress.

To import one or more group spaces:

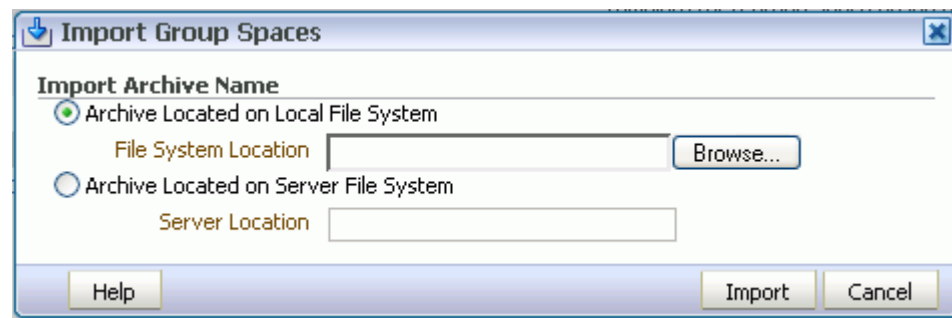
1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Group Spaces** tab.
4. Click the **Group Spaces** subtab.

Remember to take existing group spaces offline, before attempting to import a new version. For details, see [Section 22.3.1, "Taking Any Group Space Offline"](#).

5. Click **Import** in the toolbar.

The Import Group Spaces dialog box opens ([Figure 23-3](#)).

**Figure 23-3 Importing Group Spaces**



6. Specify the location of your group space archive (.ear). Select one of:
  - **Archive Located on Local File System** - Enter the **File System Location**. Alternatively, click **Browse** to locate the directory on the local file system where the .ear file is stored.
  - **Archive Located on Server File System** - Enter the **Server Location**. Any shared location accessible from this WebCenter Spaces application.

7. Click **Import**.

If you try to import a group space that already exists in the WebCenter Spaces application, you must confirm whether you want to overwrite them. To delete existing group spaces and replace them with imported versions, answer **Yes**. Answer **No** to cancel the import process.

An information message displays when all group spaces import successfully.

8. Click **Close** to dismiss the Import Group Space window.

Imported group spaces are *offline* initially because, in most cases, some additional work is required before they are ready for general use. For example, you may want to migrate data associated with back-end components. For details, see:

[Section 16.1.7.2, "Importing Discussions for a Group Space"](#)

[Section 16.1.7.4, "Importing Wikis and Blogs for a Group Space"](#)

### Section 16.1.7.5, "Exporting Documents for a Group Space"

Once content and membership details are finalized you may bring the group space online, see [Section 22–4, "Bringing a Group Space Online"](#).

## 23.3 Exporting Group Space Templates

WebCenter Spaces administrators can export group space templates and import them into other WebCenter Spaces applications. Out-of-the-box templates, such as the Group Project and Community of Interest templates, cannot be exported.

While export and import utilities are primarily used to move information between WebCenter Spaces applications, the group space template export feature is also useful as a backup service, and for sharing and exchanging templates with others.

Group space template information is exported into a single export archive (.ear file). The EAR file contains a metadata archive (.MAR file) and a single XML file containing group space security policy information.

You can save export archives to your local file system or to a remote server file system.

WebCenter Spaces administrators can export group space templates through WebCenter Spaces Administration as described here. Fusion Middleware administrators can also export group space templates using WLST commands. For details, see [Section 16.1.11.2, "Exporting Group Space Templates Using WLST"](#),

---



---

**Note:** You can also export group space information but this is a separate process. For details, see [Section 23.1, "Exporting Group Spaces"](#). You cannot export group spaces and group space templates into a single archive.

---

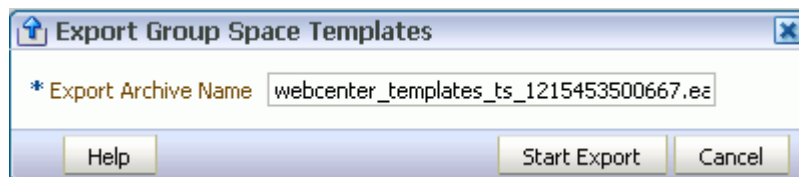


---

To export one or more group spaces templates using WebCenter Spaces:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Group Spaces** tab.
4. Click the **Templates** subtab.
5. Select the group space templates required by highlighting the row in the table.  
To select multiple group space templates, **Ctrl-click** the document rows.
6. Click **Export** on the toolbar.  
The Export Group Space Template dialog box opens ([Figure 23–4](#)).

**Figure 23–4** Exporting Group Space Templates



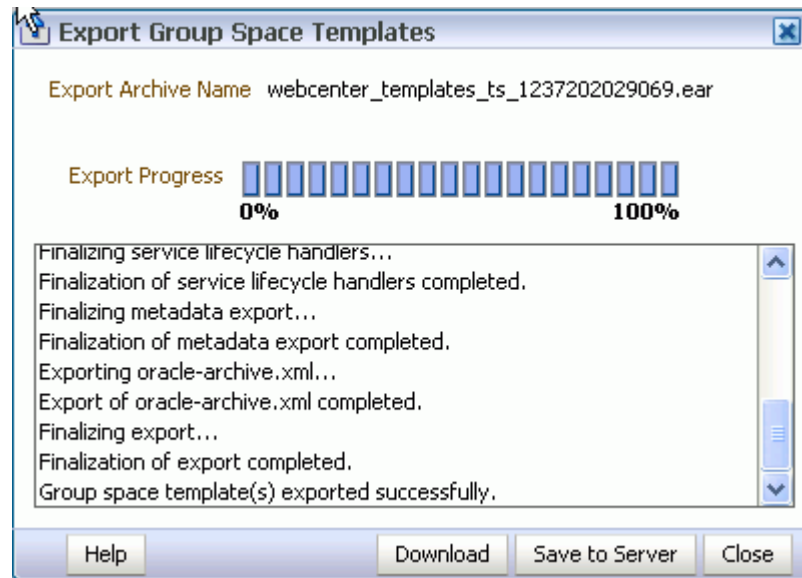
7. Change the **Export Archive Name** or accept the default name.

To ensure uniqueness, the default .ear filename contains a timestamp:  
webcenter\_templates\_ts\_<timestamp>.ear

**8. Click Start Export.**

Progress information is displayed during the export process (Figure 23–5).

**Figure 23–5 Exporting Group Space Templates In Progress**



**9. When the export process is complete, specify a location for the export archive (.ear). Select one of:**

- **Download** - Saves the export EAR file to your local file system.  
Your Browser downloads and save the archive locally. The actual download location depends on your Browser set up.
- **Save to Server** - Saves the export .ear file to a server location. For example, /tmp. Ensure that there are write permissions on the sever directory that you specify.

After clicking **Save to Server**, enter the **Server Location** and then click **Save**.

**10. Click Close** to dismiss the Export Group Space Templates window.

The export archive (.ear) is saved to the specified location.

## 23.4 Importing Group Space Templates

WebCenter Spaces administrators can import a group space template archive (.ear) into another WebCenter Spaces application.

On import, *all* group space templates included in the archive are re-created on the target application. If a group space template exists on the target, then it is deleted and replaced. If a group space template does not exist, then it is created.

Newly imported group space templates are not immediately published for general use. To learn how to make imported templates available to everyone, see [Section 22.6, "Publishing and Unpublishing Group Space Templates"](#).

WebCenter Spaces administrators can import group space templates through WebCenter Spaces Administration as described here. Fusion Middleware administrators can also import group space templates using WLST commands. For details, see [Section 16.1.11.2, "Exporting Group Space Templates Using WLST"](#),

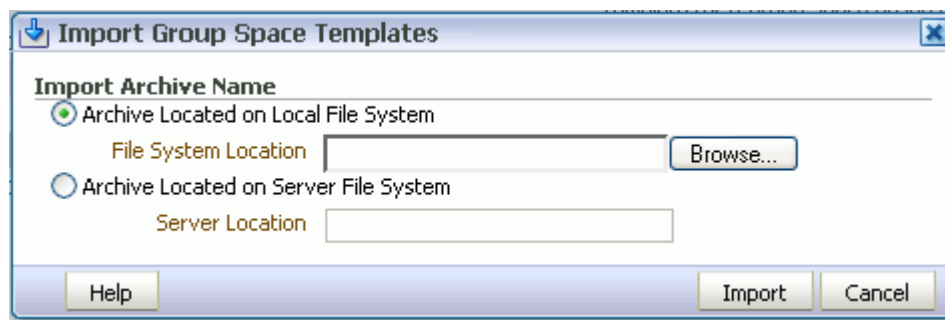
WebCenter Spaces does not support concurrent import operations. To avoid potential conflicts, import operations are disallowed while an import is in progress.

To import one or more group space templates using WebCenter Spaces:

1. Login to WebCenter Spaces with administrative privileges.  
See [Section 17.1, "Logging into WebCenter Spaces as an Administrator"](#).
2. Click the **Administration** link at the top of the application.
3. Click the **Group Spaces** tab.
4. Click the **Templates** subtab.
5. Click **Import** on the toolbar.

The Import Group Space Templates dialog box opens ([Figure 23–6](#)).

**Figure 23–6 Importing Group Space Templates**



6. Specify the location of your group space template archive (.ear). Select one of:
  - **Archive Located on Local File System** - Enter the **File System Location**. Alternatively, click **Browse** to locate the directory on the local file system where the .EAR file is stored.
  - **Archive Located on Server File System** - Enter the **Server Location**. Any shared location accessible from this WebCenter Spaces application.
7. Click **Import**.

If you try to import a group space template that already exists in the WebCenter Spaces application, you must confirm whether you want to continue. To delete existing group space templates and replace them with imported versions, answer **Yes**. Answer **No** to cancel the import process.

An information message displays when all templates import successfully.

8. Click **Close** to dismiss the Import Group Space Templates window.

To make imported templates available to everyone, see [Section 22.6, "Publishing and Unpublishing Group Space Templates"](#).

# Part VI

---

## Appendixes

Part V contains the following:

- [Appendix A, "WebCenter Configuration"](#)
- [Appendix B, "Troubleshooting"](#)





---

---

# WebCenter Configuration

The main configuration files for Oracle WebCenter applications are `adf-config.xml` and `connections.xml`. This appendix describes both these files, how to locate them in a WebCenter application deployment, as well as when to configure these files and which tools to use. Other configuration files, such as `web.xml`, are described here too. See also, [Section 1.3.4, "Oracle WebCenter Configuration Considerations."](#)

This appendix also outlines how to tune configuration properties for the operating system on which WebCenter applications are installed, WebCenter applications, and their back-end components.

This appendix includes the following sections:

- [Configuration Files](#)
  - [adf-config.xml and connections.xml](#)
  - [web.xml](#)
- [Cluster Configuration](#)
- [Configuration Tools](#)
- [Tuning Environment Configuration](#)
- [Tuning WebCenter Application Configuration](#)
- [Tuning Back-End Component Configuration](#)

## A.1 Configuration Files

`adf-config.xml`, `connections.xml`, and `web.xml` are used to configure WebCenter applications and their back-end services. This section describes how WebCenter applications use each file and the location of these files post deployment. This section includes the following sub sections:

- [adf-config.xml and connections.xml](#)
- [web.xml](#)

### A.1.1 adf-config.xml and connections.xml

`adf-config.xml` and `connections.xml` both store design time configuration information, such as the discussions server, mail server, or Oracle Content Server that is used by the WebCenter application in the development environment:

- **adf-config.xml** - Stores application-level settings, such as the which discussions server or mail server the WebCenter application is currently using.

See also, *Oracle Fusion Middleware Fusion Developer's Guide for Oracle Application Development Framework*.

- **connections.xml** - Stores connection details for WebCenter services.

See also, *Oracle Fusion Middleware Fusion Developer's Guide for Oracle Application Development Framework*.

After you deploy a WebCenter application to a production environment, you can use Fusion Middleware Control or WLST commands to reconfigure some properties to meet your production requirements. For example, you can modify connection details to point to production server instances.

Any configuration changes that you make, post deployment, are stored as *customizations* in the WebCenter application's Oracle Metadata Services (MDS) repository. MDS uses the original deployed versions of `adf-config.xml` and `connections.xml` as base documents and stores all subsequent customizations separately into MDS using a single customization layer.

When a WebCenter application starts up, customizations stored in MDS are applied to the appropriate base documents and the WebCenter application uses the merged documents (base documents with customizations) as the final set of configuration properties.

For information on MDS customizations, see "Understanding the MDS Repository" in *Oracle Fusion Middleware Administrator's Guide*.

### Locating Base Documents

`adf-config.xml` and `connections.xml` are both located in the `/META-INF` folder for your application. In a WebCenter application deployment (.ear), you will find the base documents of these files under:

```
Domain_Home/servers/server_name
```

For example, if the Domain\_Home is `ORACLE_HOME/wlshome/user_projects/domains/wc_domain/`, both configuration files are located under `ORACLE_HOME/wlshome/user_projects/domains/wc_domain/servers/WLS_Spaces`.

To determine the exact location, search for the configuration file under this folder. For example, enter the following at a command prompt:

```
> cd ORACLE_HOME/wlshome/user_projects/domains/wc_
domain/servers/WLS_Spaces
> find . -name adf-config.xml
```

A sample response, for this particular example, is as follows: `./tmp/_WL_
user/webcenter/8gco54/adf/META-INF/adf-config.xml`

You can locate `connections.xml` in a similar way.

### Reviewing Post Deployment Customizations in MDS

Post deployment, always use Fusion Middleware Control or WLST commands to review the latest configuration or make configuration changes. In Fusion Middleware Control you will mostly use WebCenter application configuration screens but a useful Systems MBean Browser is also available for reviewing configuration settings. These tools always show you the current configuration so, typically, there is no need for you to examine or change the content of base documents or MDS customization data for files such as `adf-config.xml` and `connections.xml`.

At times it might be useful to 'see' the information in MDS. If for any reason you must extract or examine configuration file customizations that are stored in MDS, use the WLST command `exportMetadata`.

---

**See also:** For detailed syntax and examples, see "exportMetadata" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

---

For example, to determine MDS customizations for `connections.xml` in WebCenter Spaces, where application name is always `webcenter`, the managed server is always `WLS_Spaces`, and the file name and location is always `/META-INF/mdssys/cust/adfshare/adfshare/connections.xml.xml`, you might specify:

```
exportMetadata(application='webcenter', server='WLS_Spaces',
toLocation='/tmp/mydata',
docs='/META-INF/mdssys/cust/adfshare/adfshare/connections.xml.xml')
```

And similarly, to determine MDS customizations for `adf-config.xml`:

```
exportMetadata(application='webcenter', server='WLS_Spaces',
toLocation='/tmp/mydata',
docs='/META-INF/mdssys/cust/adfshare/adfshare/adf-config.xml.xml')
```

You choose where to save file customizations by specifying `toLocation`. If, for example, `toLocation` is set to `/tmp/mydata`, then the requested file is saved to `/tmp/mydata/META-INF/mdssys/cust/adfshare/adfshare`.

If no customizations exist for the requested file, then nothing is saved to the specified location—previously extracted customizations at the same location are not overwritten.

### Handling Configuration Conflicts

MDS customizations use references to elements in the base document to call out which elements must be inserted/deleted/replaced, and at what location. If an element is inadvertently removed from a future redeployment and MDS contains a reference to that element, then the WebCenter application's configuration appears corrupt. You are unlikely to face this problem but should a previously deployed application appear corrupt after making changes to `adf-config.xml` or `connections.xml` you have the following options:

- Delete MDS customizations for `adf-config.xml` or `connections.xml`, deploy the new EAR file, and reconfigure your application from scratch using Fusion Middleware Control or WLST.

See below for detailed steps, "[Deleting MDS Customizations for adf-config.xml or connections.xml](#)".

- Redeploy the EAR file on a new partition or a partition where older customizations are deleted. In either case, all data previously stored in MDS for the application is lost, including any customizations for `adf-config.xml` or `connections.xml`, and all user personalizations. You must reconfigure your application from scratch too, using Fusion Middleware Control or WLST.

See also, "deleteMetadata" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

### Deleting MDS Customizations for `adf-config.xml` or `connections.xml`

1. Delete customizations for `connections.xml`, using WLST. For example:
 

```
deleteMetadata(application='webcenter', server='WLS_Spaces',
docs='/META-INF/mdssys/cust/adfshare/adfshare/connections.xml.xml')
```
2. Delete customizations for `adf-config.xml`, using WLST. For example:
 

```
deleteMetadata (application='webcenter', server='WLS_Spaces',
docs='/META-INF/mdssys/cust/adfshare/adfshare/adf-config.xml.xml')
```
3. Restart the WebCenter application.
4. Reconfigure your application from scratch using Fusion Middleware Control or WLST.

## A.1.2 web.xml

`web.xml` is a standard J2EE application deployment descriptor file and it is located in the `/META-INF` directory for your application. Typical run-time settings in `web.xml` include initialization parameters, custom tag library locations, and security settings.

Unlike `connections.xml` and `adf-config.xml`, `web.xml` does *not* store post deployment customizations in MDS.

### Locating web.xml

To determine the exact location of `web.xml` in a particular WebCenter application deployment, search for the configuration file under:

```
Domain_Home/servers/server_name
```

For example, if the `Domain_Home` is `ORACLE_HOME/wlshome/user_projects/domains/wc_domain/`, `web.xml` is located under `ORACLE_HOME/wlshome/user_projects/domains/wc_domain/servers/WLS_Spaces`.

For example, enter the following at a command prompt:

```
> cd ORACLE_HOME/wlshome/user_projects/domains/wc_
domain/servers/WLS_Spaces
> find . -name web.xml
```

A sample response, for this particular example, is as follows:

```
./tmp/_WL_user/webcenter/8gco54/adf/META-INF/web.xml
```

### Editing web.xml

You cannot use Fusion Middleware Control or WLST to modify `web.xml` in an existing WebCenter application deployment. If you must modify settings in `web.xml` you will have to do so manually, as described in [Appendix A.3.2, "Editing Configuration Files Manually"](#).

There are several instances where you might be required to modify `web.xml`, for example, if you must change:

- **Content repository upload parameters:** `UPLOAD_MAX_MEMORY`, `UPLOAD_MAX_DISK_SPACE`, and `UPLOAD_TEMP_DIR`. For details, see [Section 10.9, "Changing the Maximum File Upload Size"](#).
- **Time after which HTTP sessions expire.** For details, see [Appendix A.5.1, "Setting HTTP Session Timeout"](#).

- **JSP page timeout value.** For details, see [Appendix A.5.2, "Setting JSP Page Timeout"](#).

## A.2 Cluster Configuration

All post deployment configuration through Fusion Middleware Control, WLST, or the Systems MBean Browser is stored as customizations in the MDS repository. In a cluster environment, all configuration changes are visible to all nodes in the cluster. To effect configuration changes that are not dynamic, all nodes in the cluster must be restarted. See also [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Application Deployments"](#).

In WebCenter applications most configuration changes that you make, through Fusion Middleware Control or using WLST, are not dynamic. For example, when you add or modify connection details for Web 2.0 services (Announcements, Discussions, Documents, Mail, Instant Messaging and Presence, Search, Worklists) you must restart the application's managed server.

There are several exceptions; portlet producer and external application registration is dynamic. Any new portlet producers and external applications that you register are immediately available in your WebCenter application and any changes that you make to existing connections take effect immediately too.

If you edit configuration file manually in a cluster environment, then you must ensure that identical changes are made in each cluster member so that the overall cluster configuration remains synchronized.

## A.3 Configuration Tools

Oracle offers a range of tools for configuring WebCenter application deployments. This section outline which tools are available and in case you cannot use these tools, describes how to edit configuration files manually.

---

---

**Note:** Most of the WebCenter configuration parameters are immutable and cannot be changed at run time unless otherwise specified.

---

---

This section includes the following sub sections:

- [Configuration Through Fusion Middleware Control, WLST Commands, and System MBeans Browser](#)
- [Editing Configuration Files Manually](#)

### A.3.1 Configuration Through Fusion Middleware Control, WLST Commands, and System MBeans Browser

Post deployment, always use Fusion Middleware Control or WLST commands to review the latest configuration or make configuration changes. In Fusion Middleware Control you will mostly use WebCenter application configuration screens but a useful Systems MBean Browser is also available for reviewing and modifying configuration settings.

For more information about these tools, read:

- [Oracle Enterprise Manager Fusion Middleware Control Console](#)

- [Oracle WebLogic Scripting Tool \(WLST\)](#)
- Oracle System MBean Browser

These tools always show you the current configuration so, typically, there is no need for you to examine or manually change the content of configuration files or MDS customization data for files such as `adf-config.xml` or `connections.xml`.

If you must edit these files directly, to set concurrency options for example, follow instructions in [Appendix A.3.2, "Editing Configuration Files Manually"](#) carefully.

### A.3.2 Editing Configuration Files Manually

A few configuration settings, such as those stored in `web.xml`, are not exposed through MBeans, and therefore, you cannot use Fusion Middleware Control, WLST commands, or the System MBeans Browser for post deployment configuration.

If you must modify these settings, Oracle recommends that you re-create the WebCenter application deployment `.ear` file with the desired configuration, and redeploy the application. Sometimes this is not feasible or desirable—maybe you do not have access to the `.ear` file, or perhaps you must configure properties uniquely based on where the file is deployed—in this case, follow the manual steps below, using WLST:

1. Prevent the Weblogic Server from re-staging the WebCenter application, except at deployment time. From the WLST shell, type:

```
connect()
edit()
startEdit()
cd("DeploymentConfiguration/<domain_name>")
cmo.setRestageOnlyOnRedeploy(true)
activate()
```

2. Open the configuration file in a text editor and modify configuration properties manually, as required.

Read [Locating Base Documents](#) to find out how to determine the exact location of `adf-config.xml`, `connections.xml`, or `web.xml`.

3. Restart the managed server on which the WebCenter application is deployed.

See, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

---

---

**Caution:** If you redeploy the WebCenter application in the future you must edit the configuration file again.

---

---

## A.4 Tuning Environment Configuration

This section describes how to tune the operating system on which WebCenter applications are deployed. It provides information on configuring system limit, JDBC data source, and JRockit virtual machine (JVM) arguments.

### A.4.1 Setting System Limit

To run a WebCenter application at moderate load, set the `open-files-limit` to 4096. If you encounter errors, such as **running out of file descriptors**, then increase the system limit.

For example, on Linux, you can use this command:

```
ulimit -n 8192
```

Refer to your operating system documentation to find out how to change this system limit.

## A.4.2 Setting JDBC Data Source

The following data source settings are recommended for MDSDS and WebCenterDS. These settings can be adjusted depending on the application's usage pattern and load.

```
<jdbc-connection-pool-params>
  <initial-capacity>10</initial-capacity>
  <max-capacity>200</max-capacity>
  <capacity-increment>1</capacity-increment>
  <shrink-frequency-seconds>0</shrink-frequency-seconds>
  <highest-num-waiters>2147483647</highest-num-waiters>

<connection-creation-retry-frequency-seconds>0</connection-creation-retry-frequency-seconds>

<connection-reserve-timeout-seconds>60</connection-reserve-timeout-seconds>
  <test-frequency-seconds>0</test-frequency-seconds>
  <test-connections-on-reserve>true</test-connections-on-reserve>

<ignore-in-use-connections-enabled>true</ignore-in-use-connections-enabled>

<inactive-connection-timeout-seconds>0</inactive-connection-timeout-seconds>
  <test-table-name>SQL SELECT 1 FROM DUAL</test-table-name>
  <login-delay-seconds>0</login-delay-seconds>
  <statement-cache-size>50</statement-cache-size>
  <statement-cache-type>LRU</statement-cache-type>
  <remove-infected-connections>true</remove-infected-connections>

<seconds-to-trust-an-idle-pool-connection>60</seconds-to-trust-an-idle-pool-connection>
  <statement-timeout>-1</statement-timeout>
  <pinned-to-thread>>false</pinned-to-thread>
</jdbc-connection-pool-params>
```

To edit JDBC data source settings:

1. Login to WebLogic Server Administration Console.
2. From the Home page, select **Summary of JDBC Data Sources, Settings for mds-SpacesDS**, and then the **Connection Pool** tab.
3. Edit properties, as required.

See also "Configuring JDBC Data Sources" in *Oracle Fusion Middleware Configuring and Managing JDBC for Oracle WebLogic Server*.

## A.4.3 Setting JRockit Virtual Machine (JVM) Arguments

JVM arguments are set in the `setDomainEnv.sh` file.

- **WebLogic Server production mode:** To enable WebLogic Server production mode through WebLogic Administration Console, see *Oracle Fusion Middleware Configuring Server Environments for Oracle WebLogic Server*. The parameter is:

```
-Dweblogic.ProductionModeEnabled=true
```

- **Heap size:** If the system is overloaded, that is, garbage is collected or out of memory error occurs frequently, then increase the heap size as appropriate to your system's available physical memory. The parameter is:

```
-Xms2048M -Xmx2048M -Xns512M
```

- **Garbage collector behavior:** To maximize throughput in an application, set the following JVM option for the application's garbage collector behavior:

```
-Xgcprio:throughput -Djrockit.codegen.newlockmatching=true
```

This is an out-of-the-box setting.

- **Security:** The following JVM arguments improve performance of WebCenter application's security layer. These are out-of-box settings.

```
-DUSE_JAAS=false -Djps.policystore.hybrid.mode=false  
-Djps.combiner.optimize.lazyeval=true  
-Djps.combiner.optimize=true -Djps.auth=ACC
```

- **Log output:** This option reduces the log output in some WebCenter application-dependent components. This is an out-of-box setting:

```
-Djbo.debugoutput=silent
```

## A.5 Tuning WebCenter Application Configuration

This section describes parameters that enable administrators to tune performance of WebCenter applications.

This section includes the following:

- [Setting HTTP Session Timeout](#)
- [Setting JSP Page Timeout](#)
- [Setting ADF Client State Token](#)
- [Setting MDS Cache Size and Purge Rate](#)
- [Configuring Concurrency Management](#)
- [Configuring CRUD APIs \(Create, Read, Update and Delete\)](#)

### A.5.1 Setting HTTP Session Timeout

To manage over resource usage, adjust the session timeout value, in minutes, in the `web.xml` file.

If you must modify this property, post deployment, you must edit `web.xml` manually. See [Appendix A.3.2, "Editing Configuration Files Manually"](#).

The following is a sample snippet of `web.xml`:

```
<session-config>  
  <session-timeout>  
    45  
  </session-timeout>  
</session-config>
```



## A.5.2 Setting JSP Page Timeout

You can specify an integer value, in seconds, after which any JSP page will be removed from memory if it has not been requested in the `web.xml` file. This frees up resources in situations where some pages are called infrequently.

Increasing the value reduces user response time, and decreasing it reduces application memory footprint. The default value is 0, for no timeout.

If you must modify this property, post deployment, you must edit `web.xml` manually. See [Appendix A.3.2, "Editing Configuration Files Manually."](#)

The following is a sample snippet of `web.xml`:

```
<servlet>
  <servlet-name>
    oraclejsp
  <init-param>
    <param-name>
      jsp_timeout
    </param-name>
    <param-value>
      600
    </param-value>
  </init-param>
```

## A.5.3 Setting ADF Client State Token

Through this setting, you can control the number of pages users can navigate using the browser Back button without losing information. To reduce CPU and memory usage, you can decrease the value in the `web.xml` file.

If you must modify this property, post deployment, you must edit `web.xml` manually. See [Appendix A.3.2, "Editing Configuration Files Manually."](#)

The following is a sample snippet of `web.xml`:

```
<context-param>
  <param-name>
    org.apache.myfaces.trinidad.CLIENT_STATE_MAX_TOKENS
  </param-name>
  <param-value>
    3
  </param-value>
</context-param>
```

## A.5.4 Setting MDS Cache Size and Purge Rate

The default MDS cache size is 100MB. If you encounter the error message, **JOC region full**, then you can increase the MDS cache size in the `adf-config.xml` file.

Post deployment, modify these properties through the System MBeans Browser. For more information, see the section "Changing MDS Configuration Attributes for Deployed Applications" in *Oracle Fusion Middleware Administrator's Guide*.

The following is a sample snippet of `adf-config.xml`:

```
<cache-config>
<max-size-kb>150000</max-size-kb>
</cache-config>
```

MDS purges old version of metadata automatically every hour. If excessive metadata is accumulated and each purge is very expensive, reduce this interval in the `adf-config.xml` file.

The following is a sample snippet of `adf-config.xml`:

```
<auto-purge seconds-to-live="3600"/>
```

## A.5.5 Configuring Concurrency Management

Concurrency management includes global settings that impact entire WebCenter and service- and resource-specific settings that only impact a particular service.

You can define deployment-specific overrides or additional configuration in the `adf-config.xml` file. For example, you can specify resource-specific (producers) values that are appropriate for a particular deployment.

If you must modify these properties, post deployment, you must edit `adf-config.xml` manually. See [Appendix A.3.2, "Editing Configuration Files Manually."](#)

The following describes the format of the global, service, and resource entries in `adf-config.xml`:

```
<concurrent:adf-service-config
  xmlns="http://xmlns.oracle.com/webcenter/concurrent/config">
  <global
    queueSize="SIZE"
    poolCoreSize="SIZE"
    poolMaxSize="SIZE"
    poolKeepAlivePeriod="TIMEPERIOD"
    timeoutMinPeriod="TIMEPERIOD"
    timeoutMaxPeriod="TIMEPERIOD"
    timeoutDefaultPeriod="TIMEPERIOD"
    timeoutMonitorFrequency="TIMEPERIOD"
    hangMonitorFrequency="TIMEPERIOD"
    hangAcceptableStopPeriod="TIMEPERIOD" />
  <service
    service="SERVICENAME"
    timeoutMinPeriod="TIMEPERIOD"
    timeoutMaxPeriod="TIMEPERIOD"
    timeoutDefaultPeriod="TIMEPERIOD" />
  <resource
    service="SERVICENAME"
    resource="RESOURCENAME"
    timeoutMinPeriod="TIMEPERIOD"
    timeoutMaxPeriod="TIMEPERIOD"
    timeoutDefaultPeriod="TIMEPERIOD" />
</concurrent:adf-service-config>
```

Where:

**SIZE:** A positive integer. For example: 20.

**TIMEPERIOD:** Any positive integer followed by a suffix indicating the time unit, which must be one of: `ms` for milliseconds, `s` for seconds, `m` for minutes, or `h` for hours. For example: `50ms`, `10s`, `3m`, or `1h`. The following are examples of default settings for different services. These settings are overwritten with any service-specific configurations in `connections.xml` or `adf-config.xml` files:

```
<concurrent:adf-service-config
  xmlns="http://xmlns.oracle.com/webcenter/concurrent/config">
  <resource service="oracle.webcenter.community">
```

```

        resource="oracle.webcenter.doclib"
        timeoutMinPeriod="2s" timeoutMaxPeriod="10s" timeoutDefaultPeriod="5s"/>
<resource service="oracle.webcenter.community"
    resource="oracle.webcenter.collab.calendar.community"
    timeoutMinPeriod="2s" timeoutMaxPeriod="10s" timeoutDefaultPeriod="5s"/>
<resource service="oracle.webcenter.community"
    resource="oracle.webcenter.collab.rtc"
    timeoutMinPeriod="2s" timeoutMaxPeriod="10s" timeoutDefaultPeriod="5s"/>
<resource service="oracle.webcenter.community"
    resource="oracle.webcenter.list"
    timeoutMinPeriod="2s" timeoutMaxPeriod="10s" timeoutDefaultPeriod="5s"/>
<resource service="oracle.webcenter.community"
    resource="oracle.webcenter.collab.tasks"
    timeoutMinPeriod="2s" timeoutMaxPeriod="10s" timeoutDefaultPeriod="5s"/>
</concurrent:adf-service-config>

```

---

**Note:** All of the attributes except `service` and `resource` are optional, and therefore, for example, the following tags are valid:

```

<global queueSize="20"/>
    <resource service="foo" resource="bar" timeoutMaxPeriod="5s"/>

```

---

### A.5.6 Configuring CRUD APIs (Create, Read, Update and Delete)

CRUD API configuration for WebCenter update is defined in the `adf-config.xml` file. You can adjust the timeout to manage overall resource usage.

If you must modify these properties, post deployment, you must edit `adf-config.xml` manually. See [Appendix A.3.2, "Editing Configuration Files Manually."](#)

The following is a sample snippet of `adf-config.xml`:

```

<!-- The following entry configures the timeout for Webcenter Application CRUD
APIs -->
<concurrent:service service="oracle.webcenter.community" timeoutMinPeriod="100ms"
timeoutMaxPeriod="4s" timeoutDefaultPeriod="2s"/>
<!-- Webcenter Application configuration END -->

```

## A.6 Tuning Back-End Component Configuration

This section describes performance configuration for back-end services used by WebCenter applications. Performance of back-end servers, for example, Worklists, Oracle Content Server, and so on, should be tuned as described in guidelines for those back-ends.

This section includes the following sub sections:

- [Tuning Performance of the Announcements Service](#)
- [Tuning Performance of the Discussions Service](#)
- [Tuning Performance of the IMP Service](#)
- [Tuning Performance of the Mail Service](#)
- [Tuning Performance of the RSS News Feed Service](#)
- [Tuning Performance of the Search Service](#)
- [Tuning Performance of WSRP Producers](#)

- [Tuning Performance of Oracle PDK-Java Producers](#)
- [Tuning Performance of OmniPortlet](#)
- [Tuning Performance of the Portlet Service](#)
- [Configuring Portlet Cache Size](#)
- [Configuring Portlet Timeout](#)

### A.6.1 Tuning Performance of the Announcements Service

To manage overall resource usage for the Announcements service, you can tune the Connection Timeout property:

- Default: 10 seconds
- Minimum: 0 seconds
- Maximum: 45 seconds

Post deployment, modify the Connection Timeout property through Fusion Middleware Control or using WLST. For details, see:

- [Section 11.1.5.1, "Modifying Discussion Server Connection Details Using Fusion Middleware Control"](#)
- [Section 11.1.5.2, "Modifying Discussion Server Connection Details Using WLST"](#)

The following is a sample snippet of `connections.xml`:

```
<Reference name="Jive-7777"
className="oracle.adf.mbean.share.connection.webcenter.Announcement.
AnnouncementConnection">
<Factory
className="oracle.adf.mbean.share.connection.webcenter.forum.ForumConnectionFactory" />
    <StringRefAddr addrType="connection.time.out">
        <Contents>5</Contents>
    </StringRefAddr>
</RefAddresses>
</Reference>
```

### A.6.2 Tuning Performance of the Discussions Service

To manage overall resource usage for the Discussions service, you can tune the Connection Timeout property:

- Default: 10 seconds
- Minimum: 0 seconds
- Maximum: 45 seconds

Post deployment, modify the Connection Timeout property through Fusion Middleware Control or using WLST. For details, see:

- [Section 11.1.5.1, "Modifying Discussion Server Connection Details Using Fusion Middleware Control"](#)
- [Section 11.1.5.2, "Modifying Discussion Server Connection Details Using WLST"](#)

The following is a sample snippet of `connections.xml`:

```
<Reference name="Jive-7777"
className="oracle.adf.mbean.share.connection.webcenter.forum.ForumConnection">
    <Factory
```

```

className="oracle.adf.mbean.share.connection.webcenter.forum.ForumConnectionFactory" />
  <RefAddresses>
    <StringRefAddr addrType="forum.url">
      <Contents>http://[machine]:[port]/owc_discussions_5520</Contents>
    <StringRefAddr addrType="connection.time.out">
      <Contents>5</Contents>
    </StringRefAddr>
  </RefAddresses>
</Reference>

```

### A.6.3 Tuning Performance of the IMP Service

To manage overall resource usage for the IMP service, you can tune the Connection Timeout property:

- Default: 10 seconds
- Minimum: 0 seconds
- Maximum: 45 seconds

Post deployment, modify the Connection Timeout property through Fusion Middleware Control or using WLST. For details, see:

- [Section 11.2.5.1, "Modifying Instant Messaging and Presence Connections Details Using Fusion Middleware Control"](#)
- [Section 11.2.5.2, "Modifying Instant Messaging and Presence Connections Details Using WLST"](#)

The following is a sample snippet of `connections.xml`:

```

<Reference name="IMPService-OWLCS"
  className="oracle.adf.mbean.share.connection.webcenter.rtc.RtcConnection">
  <Factory
className="oracle.adf.mbean.share.connection.webcenter.rtc.RtcConnectionFactory" />
  <RefAddresses>
    <StringRefAddr addrType="connection.time.out">
      <Contents>5</Contents>
    </StringRefAddr>
  </RefAddresses>
</Reference>

```

### A.6.4 Tuning Performance of the Mail Service

To manage overall resource usage for the Mail service, you can tune the Connection Timeout property:

- Default: 10 seconds
- Minimum: 0 seconds
- Maximum: 45 seconds

Post deployment, modify the Connection Timeout property through Fusion Middleware Control or using WLST. For details, see:

- [Section 11.3.5.1, "Modifying Mail Server Connection Details Using Fusion Middleware Control"](#)
- [Section 11.3.5.2, "Modifying Mail Server Connection Details Using WLST"](#)

The following is a sample snippet of `connections.xml`:

```

<Reference name="MailConnection"
className="oracle.adf.mbean.share.connection.webcenter.mail.MailConnection">
  <StringRefAddr addrType="connection.time.out">
    <Contents>5</Contents>
  </StringRefAddr>
</Reference>

```

## A.6.5 Tuning Performance of the RSS News Feed Service

To manage overall resource usage for the RSS News Feed service, you can adjust the refresh interval and timeout in the `adf-config.xml` file.

If you must modify these properties, post deployment, use the System MBeans Browser.

The following is a sample snippet of `adf-config.xml`:

```

<rssC:adf-rss-config>
  <rssC:RefreshSecs>3600</rssC:RefreshSecs>
  <rssC:TimeoutSecs>3</rssC:TimeoutSecs>
  <rssC:Configured>true</rssC:Configured>
</rssC:adf-rss-config>

```

## A.6.6 Tuning Performance of the Search Service

To manage overall resource usage and user response time for searching, you can adjust the number of saved searches displayed, the number of results displayed, and these timeout values:

- `prepareTimeoutMs` - Maximum time that a service is allowed to initialize a search (in ms).
- `timeoutMs` - Maximum time that a service is allowed to execute a search (in ms).
- `showAllTimeoutMs` - Maximum time that a service is allowed to display search all results (in ms).

Post deployment, modify timeout properties through Fusion Middleware Control or using WLST. For details, see:

- [Section 11.4.5.1, "Modifying Oracle Secure Enterprise Search \(SES\) Connection Details Using Fusion Middleware Control"](#)
- [Section 11.4.5.2, "Modifying Search Service Properties Using WLST"](#)

The following is a sample snippet of `adf-config.xml`:

```

<searchC:adf-search-config
xmlns="http://xmlns.oracle.com/webcenter/search/config">
  <display-properties>
    <common numSavedSearches="25" />
    <region-specific>
      <usage id="simpleSearchResultUIMetadata" numServiceRows="5" />
      <usage id="searchResultUIMetadata" numServiceRows="5" />
      <usage id="localToolbarRegion" numServiceRows="5" />
    </region-specific>
  </display-properties>
  <execution-properties prepareTimeoutMs="1000" timeoutMs="3000"
showAllTimeoutMs="20000" />
</execution-properties>
</searchC:adf-search-config>

```

## A.6.7 Tuning Performance of WSRP Producers

To manage overall resource usage for a WSRP producer, you can tune the Connection Timeout property:

- Default: 30000 ms
- Minimum: 5000 ms
- Maximum: 60000 ms

Post deployment, modify the Connection Timeout property through Fusion Middleware Control or using WLST. For details, see:

- [Section 12.6.1, "Editing Producer Registration Details Using Fusion Middleware Control"](#)
- [Section 12.6.2, "Editing Producer Registration Details Using WLST"](#)

The following is a sample snippet of `connections.xml`:

```
<wsrpproducerconnection producerName="wc-RichText"
wsConnection="wc-RichText-wsconn" timeout="30"/>
      <wsrpproducerconnection producerName="wc-WSRPTools"
wsConnection="wc-WSRPTools-wsconn" timeout="30"/>
```

## A.6.8 Tuning Performance of Oracle PDK-Java Producers

To manage overall resource usage for a Web producer, you can tune the Connection Timeout property:

- Default: 30000 ms
- Minimum: 5000 ms
- Maximum: 60000 ms

Post deployment, modify the Connection Timeout property through Fusion Middleware Control or using WLST. For details, see:

- [Section 12.6.1, "Editing Producer Registration Details Using Fusion Middleware Control"](#)
- [Section 12.6.2, "Editing Producer Registration Details Using WLST"](#)

The following is a sample snippet of `connections.xml`:

```
<webproducerconnection producerName="wc-WebClipping"
urlConnection="wc-WebClipping-urlconn" timeout="10000" establishSession="true"
mapUser="false"/>
```

## A.6.9 Tuning Performance of OmniPortlet

To manage overall resource usage for OmniPortlets, you can tune the Connection Timeout property:

- Default: 30000 ms
- Minimum: 5000 ms
- Maximum: 60000 ms

Post deployment, modify the Connection Timeout property through Fusion Middleware Control or using WLST. For details, see:

- [Section 12.6.1, "Editing Producer Registration Details Using Fusion Middleware Control"](#)

- [Section 12.6.2, "Editing Producer Registration Details Using WLST"](#)

The following is a sample snippet of `connections.xml`:

```
<webproducerconnection producerName="wc-OmniPortlet"
urlConnection="wc-OmniPortlet-urlconn" timeout="10000" establishSession="false"
mapUser="false"/>
```

## A.6.10 Tuning Performance of the Portlet Service

To manage overall resource usage and user response time, you can remove unnecessary locale support, modify portlet timeout and cache size in the `adf-config.xml` file.

For the Portlet service, 28 supported locales are defined out-of-the-box. You can remove the locales that are unnecessary for your application.

If you must modify these properties, post deployment, you must edit `adf-config.xml` manually. See [Appendix A.3.2, "Editing Configuration Files Manually."](#)

The following is a sample snippet of `adf-config.xml`:

```
<portletC:adf-portlet-config xmlns="http://xmlns.oracle.com/adf/portlet/config">
  <supportedLocales>
    <value>es</value>
    <value>ko</value>
    <value>ru</value>
    <value>ar</value>
    <value>fi</value>
    <value>nl</value>
    <value>sk</value>
    <value>cs</value>
    <value>fr</value>
    <value>no</value>
    <value>sv</value>
    <value>da</value>
    <value>hu</value>
    <value>pl</value>
    <value>th</value>
    <value>de</value>
    <value>it</value>
    <value>pt</value>
    <value>tr</value>
    <value>el</value>
    <value>iw</value>
    <value>pt_BR</value>
    <value>zh_CN</value>
    <value>en</value>
    <value>ja</value>
    <value>ro</value>
    <value>zh_TW</value>
  </supportedLocales>
  <defaultTimeout>20</defaultTimeout>
  <minimumTimeout>1</minimumTimeout>
  <maximumTimeout>60</maximumTimeout>
  <parallelPoolSize>10</parallelPoolSize>
  <parallelQueueSize>20</parallelQueueSize>
  <cacheSettings enabled="true">
    <maxSize>10000000</maxSize>
  </cacheSettings>
</portletC:adf-portlet-config>
```



## A.6.11 Configuring Portlet Cache Size

You can modify the portlet cache size in the `adf-config.xml` file. The default portlet cache size is set to 10 MB.

If you must modify these properties, post deployment, you must edit `adf-config.xml` manually. See [Appendix A.3.2, "Editing Configuration Files Manually."](#)

The following is a sample snippet of `adf-config.xml`:

```
<adf-portlet-config>
  ....
  <supportedLocales>
    <cacheSettings enabled="true">
      <maxSize>10000000</maxSize>
    </cacheSettings>
  </adf-portlet-config>
```

## A.6.12 Configuring Portlet Timeout

You can modify the portlet timeout value in the `adf-portlet-config` element of the `adf-config.xml` file. Default: 10 seconds, minimum: 0.1 seconds, maximum: 60 seconds.

If you must modify these properties, post deployment, you must edit `adf-config.xml` manually. See [Appendix A.3.2, "Editing Configuration Files Manually."](#)

The following is a sample snippet of `adf-config.xml`:

```
<adf-portlet-config>
  ....
  <defaultTimeout>5</defaultTimeout>
  <minimumTimeout>2</minimumTimeout>
  <maximumTimeout>100</maximumTimeout>
</adf-portlet-config>
```



---

---

## Troubleshooting

This appendix provides solutions to common issues that occur in WebCenter applications. This includes the following sections:

- [Troubleshooting WebCenter Application Configuration Issues](#)
- [Troubleshooting WLST Command Issues](#)
- [Troubleshooting Discussions Service Issues](#)
- [Troubleshooting Instant Messaging and Presence Service Issues](#)
- [Troubleshooting Mail Service Issues](#)
- [Troubleshooting Portlet Producer Issues](#)
- [Troubleshooting Wiki and Blog Issues](#)
- [Troubleshooting Worklist Service Issues](#)
- [Troubleshooting WebCenter Spaces Import and Export Issues](#)

### B.1 Troubleshooting WebCenter Application Configuration Issues

This section includes the following sub sections:

- [WebCenter Does Not Display in the Application Deployment Menu in Fusion Middleware Control](#)
- [Configuration Options Unavailable](#)
- [Configuration Performed in One Application Reflects in Another](#)

#### B.1.1 WebCenter Does Not Display in the Application Deployment Menu in Fusion Middleware Control

##### **Problem**

After logging into Fusion Middleware Control, you cannot find the **WebCenter** option in the **Application Deployment** menu.

##### **Solution**

Ensure the following:

- Deployed application is an ADF application.  
The **WebCenter** option does not display for applications that are not developed using ADF.

- Deployed application is up and running.
- Deployed application contains accurate information about MDS repository and partition, and the MDS repository is accessible to the application. To verify this, check the `metadata-store-usages` section in the `adf-config.xml` file. For information on MDS, see "Understanding the MDS Repository" in *Oracle Fusion Middleware Administrator's Guide*.
- Application is packaged with required artifacts to support configuration:
  - `adf-jndi-config` name space is configured in the application's `adf-config.xml` file. This is provisioned at design time. The following is an example (the text in **bold**) of the `adf-jndi-config` name space:

```
<adf-config xmlns="http://xmlns.oracle.com/adf/config"
  xmlns:jndiC="http://xmlns.oracle.com/adf/jndi/config"
  xmlns:ns2="http://xmlns.oracle.com/mds/config"
  xmlns:ns3="http://xmlns.oracle.com/adf/mds/config">
  ...
  ...
</adf-config>
```

- `MDSBackingStore` is configured in the application's `adf-config.xml` file. This is provisioned at design time. This section can exist anywhere in the upper `adf-config` element, for instance, after the end tag of `adf-mds-config`. For example, see the text in **bold** in the following snippet:

```
<jndiC:adf-jndi-config>
  <jndiC:ConnectionsJndiContext
initialContextFactoryClass="oracle.adf.share.jndi.InitialContextFactoryImpl"
"
backingStoreURL="META-INF/connections.xml"
backingStoreClass="oracle.adf.share.jndi.MDSBackingStore">
  <jndiC:contextEnv value="true" name="cache_application_scope"/>
  </jndiC:ConnectionsJndiContext>
</jndiC:adf-jndi-config>
```

- Appropriate listeners exist in the `web.xml` file to register the MBeans. This is provisioned at design time. For example, see the text in **bold** in the following snippet of the `web.xml` file:

```
<listener>
  <description>ADF Config MBeans</description>
  <display-name>ADF Config MBeans</display-name>

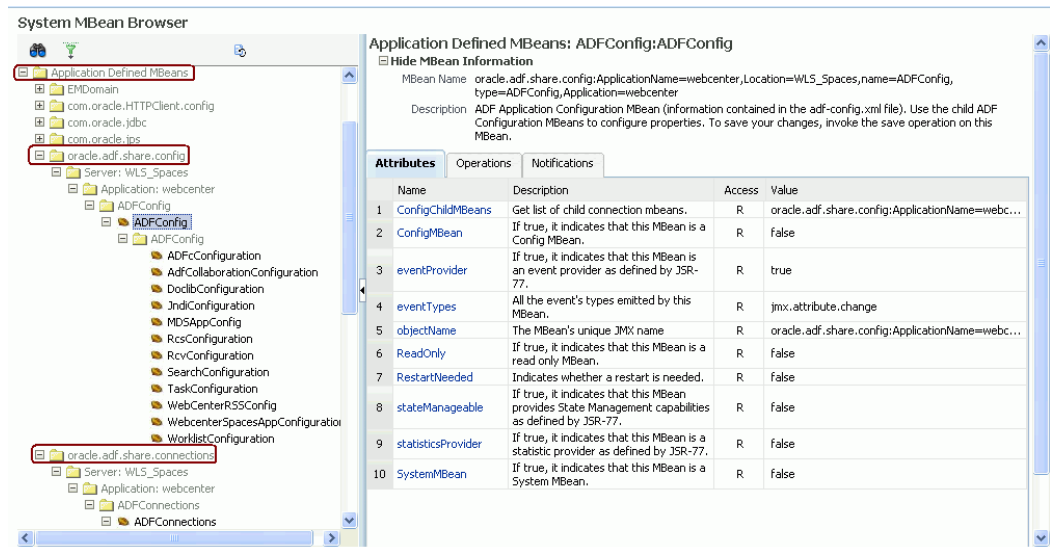
<listener-class>oracle.adf.mbean.share.config.ADFConfigLifecycleCallBack</l
istener-class>
</listener>
<listener>
  <description>ADF Connection MBeans</description>
  <display-name>ADF Connection MBeans</display-name>

<listener-class>oracle.adf.mbean.share.connection.ADFConnectionLifecycleCal
lBack</listener-class>
</listener>
```

- MBeans is registered for the WebCenter application. To verify this:
  1. In Fusion Middleware Control, from the **Application Deployment** menu, select **System MBean Browser**.

2. Locate connection MBeans for your application under **Application Defined MBeans > oracle.adf.mbean.share.connection**.
  3. Similarly, locate `adf-config` MBeans for your application under **Application Defined MBeans > oracle.adf.mbean.share.config**. [Figure B-1](#) shows how the Application Defined MBeans section looks in Fusion Middleware Control.
- If your application consumes producers, then locate the **Producer Manager** Mbean.

**Figure B-1 Application Defined MBeans**



- Check the application's diagnostic logs, analyze messages for the modules `oracle.adf.mbean.share.connection` and `oracle.adf.mbean.share.config`, and determine what must be done.

## B.1.2 Configuration Options Unavailable

### Problem

When you try to configure an application in Fusion Middleware Control, the following message displays:

Configuration options currently unavailable. The application `application_name` might be down, did not start-up properly, or is incorrectly packaged. Check the log files for further details.

### Solution

For information on how to resolve this issue, see [Section B.1.1, "WebCenter Does Not Display in the Application Deployment Menu in Fusion Middleware Control."](#)

## B.1.3 Configuration Performed in One Application Reflects in Another

### Problem

You configured a WebCenter application, but those configurations also show in another application.

**Solution**

This happens when multiple applications share the MDS partition in the same schema. To resolve this problem, deploy these applications again and ensure that each application uses its own MDS schema and partition combination. For information about creating a MDS repository or configuring an existing WebCenter application to use a different MDS repository or partition, see section "Managing the Oracle Metadata Repository" in *Oracle Fusion Middleware Administrator's Guide*.

## B.2 Troubleshooting WLST Command Issues

This section includes the following sub sections:

- [None of the WLST Commands Work](#)
- [WLST Commands Do Not Work for a Particular Service](#)
- [A Connection with the Name Connection\\_Name Already Exists](#)
- [WLST Shell is Not Connected to the Oracle WebLogic Managed Server Instance](#)
- [Application with the Same Name Already Exists in a Domain](#)
- [Application with the Same Name Already Exists on a Managed Server](#)
- [Already in Domain Runtime Tree Message Displays](#)

### B.2.1 None of the WLST Commands Work

**Problem**

You are unable to run any WLST commands.

**Solution**

Ensure the following:

- No files other than Python are stored in the WLST source directory: `ORACLE_HOME/common/bin/wlst`. This directory must contains files with the `.py` extension only.  
  
The default set of files in this location contain legal Python files from Oracle. It is possible that a user copied some non-python script to this directory, for example, a backup file or a test python file with syntax errors.
- `webcenter-wlst.jar` is located at `ORACLE_HOME/common/bin/wlst/lib`.
- WebCenter WLST files do not have syntax errors. A single file with syntax error can cause problems.

### B.2.2 WLST Commands Do Not Work for a Particular Service

**Problem**

You are unable to run WLST commands for a particular service, and therefore, you cannot configure that service.

**Solution**

First, run generic non-WebCenter commands, for example, `listApplications()` and `displayMetricTableNames()` to verify whether these commands work. If generic commands do not work, then apply the solution described in [Section B.2.1, "None of the WLST Commands Work."](#)

If generic commands work, then run test commands to check the sanity of WebCenter-specific commands. In other words, ensure that the WebCenter WLST file for that service has no syntax errors. To verify this, run the appropriate WSLT check command (see [Table B-1](#)).

See also, [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

**Table B-1 File Names and WLST Commands for Web 2.0 Services**

| Service Name                              | File Name                 | WLST Command          |
|---|---------------------------|-----------------------|
| Discussions and Announcements             | ForumWLST.py              | fcpcCheck()           |
| Documents                                 | DoclibWLST.py             | doclibCheck()         |
| External Applications                     | ExtAppWLST.py             | extCheck()            |
| Group Space Events                        | CommunityWLST.py          | ceCheck()             |
| Instant Messaging and Presence            | ImpWLST.py                | rtcCheck()            |
| Mail                                      | MailWLST.py               | mailCheck()           |
| Producer Help                             | ProducerHelperWLST.py     | producerHelperCheck() |
| WSRP Producers                            | WsrpWLST.py               | wsrpCheck()           |
| PDK Producers                             | PdkWLST.py                | pdkCheck()            |
| RSS News Feed                             | RSSWLST.py                | rssCheck()            |
| Search                                    | SesWLST.py                | sesCheck()            |
| Worklist                                  | BpelWLST.py               | bpelCheck()           |
| WebCenter Spaces and SOA                  | WebCenterSpacesSOAWLST.py | spaceCheck()          |
| Export/Import - WebCenter application     | LifecycleWLST.py          | lifecycleCheck()      |
| Export/Import - Group Spaces and Template | ExtImpWLST.py             | expimpCheck()         |
| WebCenter Help                            | WebCenterWLSTHelper.py    | basicCheck()          |

### B.2.3 A Connection with the Name `Connection_Name` Already Exists

#### Problem

You are unable to create a connection with the name `connection_name`. The following message displays:

```
A connection with name Connection_Name already exists.
```

#### Solution

Connection names are unique across WebCenter applications. This error occurs when you try to create a connection with a name that is already in use. Ensure that you use a unique name for your connection.

## B.2.4 WLST Shell is Not Connected to the Oracle WebLogic Managed Server Instance

### Problem

The WLST shell is not connected to the managed server on which you want to run WLST commands.

### Solution

Run the following command to connect the WLST shell to the managed server:

```
connect(username, password , serverhost:serverport)
```

See also, [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

## B.2.5 Application with the Same Name Already Exists in a Domain

### Problem

You are unable to register a producer application. The following message displays:

```
Another application named "YourApplicationName" exists. Specify the Server on which your application is deployed. Use: server="YourServerName".
```

### Solution

There are multiple applications with the same name in the domain in which you are trying to register your application. This usually happens in a cluster environment, where the same application is deployed to multiple managed servers. If this is the case, specify the name of the server in which you are trying to register this application. For example, run the `registerWSRPProducer` WLST command with the `server` argument:

```
registerWSRPProducer(appName='myApp', name='MyWSRPSamples',  
url='http://host:port/application_name/portlets/wsrp2?WSDL', server=server_name)
```

For command syntax and examples, see "registerWSRPProducer" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

See also, [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

## B.2.6 Application with the Same Name Already Exists on a Managed Server

### Problem

You are unable to register a producer application. The following message displays:

```
Another application named "application_name" exists on the server  
managedServerName.
```

### Solution

There are multiple applications with the same name on the managed server in which you are trying to register your application. This usually happens when applications are assigned different versions. If this is the case, specify the version of the application you want to register. For example, run the `registerWSRPProducer` WLST command with the arguments `server` and `applicationVersion`:

```
registerWSRPProducer(appName='myApp', name='MyWSRPSamples',  
url='http://host:port/application_name/portlets/wsrp2?WSDL',
```



```
server=server_name applicationVersion=version of the application)
```

For command syntax and examples, see "registerWSRPPProducer" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

See also, [Section 1.12.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

## B.2.7 Already in Domain Runtime Tree Message Displays

### Problem

While running a WLST command, the following message displays:

```
Already in Domain Runtime Tree
```

### Solution

This is a benign message, and therefore, you can ignore it.

## B.3 Troubleshooting Discussions Service Issues

This section includes the following sub sections:

- [Discussion Forum Cannot Be Enabled in Group Spaces](#)
- [Login Does Not Function Properly After Configuring OAM-SSO](#)

### B.3.1 Discussion Forum Cannot Be Enabled in Group Spaces

#### Problem

Discussion services cannot be enabled in any group space, even new group spaces.

#### Solution

This error may be caused due to various reasons. Check the following:

- Oracle WebCenter Discussions server is up and running and accessible. See, [Section 11.1.9, "Testing Discussion Server Connections."](#)
- Administrator User Name (adminUser) property configured for the active discussion connection has administrative privileges on the application root category (the category configured for the WebCenter Spaces). See [Section 11.1.3, "Registering Discussion Servers."](#)

It is not necessary for this user to be a super admin. However, the user must have administrative privileges on the application root category configured for the WebCenter Spaces, that is, the category (on the discussion server) under which all group space discussions and announcement are stored.

- Application root category, where all group space discussions and announcement are stored, exists on the back-end server.

You can check the application root category ID configured for the WebCenter Spaces application by navigating WebCenter Administration, selecting **Services**, and then **Discussions**. See, [Section 18.8.1, "Specifying Where Discussions and Announcements are Stored on the Discussions Server."](#)

## B.3.2 Login Does Not Function Properly After Configuring OAM-SSO

### Problem

When you log into the discussions server after configuring OAM-SSO, a 500 - Internal Server Error occurs.

### Solution

This error occurs if the LDAP back-end is already configured for the discussions server and you add a new `SSOAuthFactory` property to configure SSO instead of editing the existing property.

Go to the Administration page and remove LDAP `AuthFactory` and `SSOAuthFactory` properties. If needed, run the following SQL to restore the correct value:

```
insert into jiveproperty
values ('AuthFactory.className', 'oracle.jive.sso.OracleSSOAuthFactory');
```

Consider the following when configuring OAM-SSO:

- If the discussions server is not configured with the LDAP `AuthFactory` property already, then you must add a new property to configure SSO:

```
AuthFactory.className=Oracle.jive.sso.OracleSSOAuthFactory
```

- If the discussions server is already configured with an LDAP `AuthFactory`, then you must edit the `AuthFactory.className` property while configuring SSO and set it to:

```
Oracle.jive.sso.OracleSSOAuthFactory
```

## B.4 Troubleshooting Instant Messaging and Presence Service Issues

### Problem

Buddies are not visible in a custom WebCenter application. Further, the presence status of users is not available.

### Solution

Ensure the following:

- IMP connection is configured properly and the base URL and domain values are correct. See, [Section 11.2.3, "Registering Instant Messaging and Presence Servers."](#)
- Web Services for the communication server is installed properly and is up and running. For Web Services installation for Oracle WebLogic Communications Server, see the *Oracle WebLogic Communication Services Administrator's Guide*. For Web Services installation for Microsoft Live Communications Server, see [Section 11.2.2.2, "Microsoft Live Communications Server \(LCS\) Prerequisites."](#)
- Back-end communication server (Oracle WebLogic Communications Server or Microsoft Live Communications Server) is up and running. A quick way to verify this is to ensure that the user can connect to the communication server by using a supported SIP client (Oracle Communicator or Microsoft Communicator).
- User is logged in with valid user credentials and the user exists on the communication server. For Microsoft Live Communications Server, verify that user has provided correct credentials in the external application.

## B.5 Troubleshooting Mail Service Issues

This section includes the following sub sections:

- [Mail Service is Not Accessible in Secure Mode](#)
- [Mail Service is Not Accessible in Non-Secure Mode](#)
- [Unable to Create Distribution Lists in the Non-Secure Mode](#)
- [Unable to Create Distribution Lists in the Secure Mode](#)
- [Unable to Configure the Number of Mails Downloaded](#)
- [Unable to Publish and Archive Group Space Mail](#)

### B.5.1 Mail Service is Not Accessible in Secure Mode

#### Problem

You configured the Mail service to function in secure mode, but the service is not accessible.

#### Solution

Ensure the following:

- IMAP and SMTP ports are specified correctly. See [Section 11.3.3, "Registering Mail Servers."](#)
- Properties are set to `true` in your mail server.
  - `mail.imap.Secured = true`
  - `mail.smtp.Secured = true`

### B.5.2 Mail Service is Not Accessible in Non-Secure Mode

#### Problem

You configured the Mail service to function in non-secure mode, but the service is not accessible.

#### Solution

Ensure the following:

- IMAP and SMTP ports are specified correctly. See, [Section 11.3.3, "Registering Mail Servers."](#)
- Properties are set to `false` in your mail server.
  - `mail.imap.Secured = false`
  - `mail.smtp.Secured = false`

### B.5.3 Unable to Create Distribution Lists in the Non-Secure Mode

#### Problem

You are unable to create group space distribution lists in non-secure mode (SSL not configured).

### **Solution**

Check if the mail server has been reinstalled or the user has been deleted. Also ensure that the following parameters are configured accurately in non-secure mode, in the LDAP server:

- ldapHost
- defaultUser
- ldapAdminPassword
- ldapBaseDN
- ldapPort

See, [Section 11.3.3, "Registering Mail Servers."](#)

## **B.5.4 Unable to Create Distribution Lists in the Secure Mode**

### **Problem**

You are unable to create group space distribution list in secure mode, that is, SSL is configured on the LDAP server.

### **Solution**

Check if the mail server has been reinstalled or the user has been deleted. Also ensure that the following parameters are configured accurately in secure mode, in the LDAP server:

- ldapHost
- defaultUser
- ldapAdminPassword
- ldapBaseDN
- ldapPort
- ldap.connection.secure, 'true'

See, [Section 11.3.3, "Registering Mail Servers."](#)

## **B.5.5 Unable to Configure the Number of Mails Downloaded**

### **Problem**

You cannot configure how many mails are downloaded to each user's Inbox.

### **Solution**

Use the `setMailServiceProperty` WLST command. For example, to download 100 mails from the e-mail client, specify the `mail.messages.fetch.size` parameter as 100, as shown in the following example:

```
setMailServiceProperty(appName='webcenter', property='mail.messages.fetch.size',
value='100')
```

For command syntax and examples, see "setMailServiceProperty" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

## B.5.6 Unable to Publish and Archive Group Space Mail

### Problem

You are unable to archive group space mail.

### Solution

If the archiving fails, check the following:

- In WebCenter Spaces, open WebCenter Administration pages, navigate to the Services tab, and then choose Discussions. Check whether the required configuration is accurate. See also, [Section 18.8.3, "Enabling Discussion Forums to Publish Group Space Mail."](#)
- Check whether the user account configured here is a member of the distribution list.
- For a particular group space, check whether the forum configured is available in the discussion server. See "Publishing Group Space Mail in a Discussion Forum" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter*.
- Check whether the user who sends emails to the distribution list is available in the discussion server and his email address is the same.

## B.6 Troubleshooting Portlet Producer Issues

This section includes the following sub sections:

- [Producer Registration Fails for a Custom WebCenter Application](#)
- [Portlet Unavailable: WSM-00101 Exception](#)

### B.6.1 Producer Registration Fails for a Custom WebCenter Application

This section describes producer registration and portlet unavailability issues.

#### Problem

You are unable to register a WSRP producer.

#### Solution

Ensure the following:

- Back-end producer is up and running. To test the producer, access the WSDL URL of the producer through a browser window. See, [Section 12.3, "Testing WSRP Producer Connections."](#)
- Producer application is packaged accurately. If not, then register the producer at design time (in JDeveloper), as described in the section "Registering Portlet Producers with a WebCenter Application" in the chapter "Consuming Portlets" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*, and redeploy the application, as described in [Section 7.1, "Deploying Custom WebCenter Applications."](#) After redeployment, verify that the packaged application includes the MBean, `ProducerManager`:
  1. In Fusion Middleware Control, from the **Application Deployment** menu, select **System MBean Browser**.

2. In the Navigator, expand **Application Defined MBeans** > **oracle.webcenter.portlet** > **Application: *application\_name*** > **Producer Manager** > **Producer Manager**.
  - PortletServletContextListener is added to the web.xml file.

For applications that support post deployment registration of producers, the producer must be registered at least once at design time. This adds PortletServletContextListener to the web.xml file, which registers the appropriate runtime MBeans to enable post deployment registration of producers. For example, see the text in **bold** in the following web.xml snippet:

```
<listener>
  <description>
    WebCenter Portlet Context Listener
  </description>
  <display-name>
    WebCenterPortletContextListener
  </display-name>
  <listener-class>
    oracle.webcenter.portlet.listener.PortletServletContextListener
  </listener-class>
</listener>
```

## B.6.2 Portlet Unavailable: WSM-00101 Exception

Setting up the **User Name with Password** token profile in a WSRP portlet producer throws the exception WSM-00101.

### Problem

If you configure the **User Name with Password Token** profile for a WSRP producer through Fusion Middleware Control (or WLST) while portlets associated with this producer are in use, the portlets display the following exception in the WebCenter application:

```
oracle.wsm.common.sdk.WSMException: WSM-00101:
The specified Keystore file
/keys/user_projects/domains/pv_0309/config/fmwconfig/default-keystore.jks
cannot be found; it either does not exist or its path is not included in the
application classpath.
```

### Solution

Ensure that you have configured the default keystore in your portlet producer. For information, see [Section 14.8.4.3, "Setting Up the Keystores."](#)

## B.7 Troubleshooting Wiki and Blog Issues

This section describes a possible issue that you may face after configuring OAM-SSO on Oracle WebCenter Wiki and Blog Server.

### Problem

After configuring OAM-SSO on Oracle WebCenter Wiki and Blog Server when you log out, the server does not redirect to the login page properly.

**Solution**

Ensure that the `logout_url` property is set accurately in the `application_config.script` file located in the `MW_HOME/user_projects/domains/fmw_domain/servers/WLS_Services/stage/owc_wiki/11.1.1.1.0/owc_wiki/WEB-INF/` directory.

## B.8 Troubleshooting Worklist Service Issues

The Worklist service relies on several middleware components to display worklist items to logged-in users. Therefore, several factors may cause the Worklist service to fail. The issues and solutions discussed in this section relate to common problems that may be encountered.

This section includes the following sub sections:

- [Unavailability of the Worklist Service Due to Application Configuration Issues](#)
- [Unavailability of the Worklist Service Due to Server Failure](#)

---

**Note:** To identify causes of failures, examine log files on the managed servers hosting Worklist service processes and the managed servers for any SOA BPEL servers you have configured.

---

### B.8.1 Unavailability of the Worklist Service Due to Application Configuration Issues

Issues described in this section pertain to the unavailability of the Worklist service—Worklist task flows display the message **The Worklist service is unavailable** with the following warning:

Either no BPEL connections are configured, or there is an issue with the existing connection configuration. Verify that at least one BPEL Worklist connection is configured for this application, and that no unresolved "ConfigurationExceptions" exceptions are logged.

This section includes the following sub sections:

- [adf-config.xml Refers to a Non-Existent BPEL Connection](#)
- [adf-config.xml Has No Reference to a BPEL Connection](#)
- [No Rows Yet Message Displays](#)

#### B.8.1.1 adf-config.xml Refers to a Non-Existent BPEL Connection

**Problem**

The connection listed in the `adf-config.xml` file does not exist in the application's `connections.xml` file. The following entries exist in the diagnostic log file for the managed server on which the application is running:

```
[2009-03-22T13:33:54.140+00:00] [DefaultServer] [WARNING]
[WCS-32008] [oracle.webcenter.worklist.config][tid:
[ACTIVE].ExecuteThread: '12' for queue: 'weblogic.kernel.Default
(self-tuning)'] userId: user][ ecid:
0000I0iOmdTFk3FLN2o2ye19kTB0000V,0][APP: Worklist#V2.0 arg:
Human Resources The BPEL Connection named 'connection_name' was
not present in the connections.xml file. This will prevent the
```

Worklist service from being able to interact with the required this BPEL connection.

### Solution

Either create a BPEL connection with the name stated in the log, or remove the connection. For more information about how to update the Worklist configuration post deployment, see [Section 11.5, "Setting Up Connections for the Worklist Service."](#)

During development, refer to the chapter "Integrating the Worklist Service" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

To find out which connections names are referenced and to validate the Worklist service configuration, run the WLST command, `listWorklistConnections(appName='myApp', verbose=true)`. For more information, see "listWorklistConnections" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

### B.8.1.2 adf-config.xml Has No Reference to a BPEL Connection

There is no reference to a Worklist service connection in the application's `adf-config.xml`, but this connection exists in the `connections.xml` file.

### Problem

In diagnostic log files for the managed server on which the application is running, you see entries such as the following:

```
[2009-03-23T10:23:56.943+00:00] [DefaultServer] [WARNING]
[WCS-32009] [oracle.webcenter.worklist.config] [tid:
[ACTIVE].ExecuteThread: '21' for queue: 'weblogic.kernel.Default
(self-tuning)'] [userId: user] [ecid:
0000I0mqx8Fk3FLN2o2ye19lqBV000008,0] [APP: Worklist#V2.0] The
Worklist service does not have a ConnectionName configuration
entry in adf-config.xml that maps to a BPELConnection in
connections.xml, therefore the Worklist service was not
configured for this application.
```

### Solution

Configure a connection to at least one BPEL server so that the Worklist service can query worklist items.

Post deployment, create Worklist connections through WLST or Fusion Middleware Control. For information, see [Section 11.5, "Setting Up Connections for the Worklist Service."](#) During development, create Worklist connections through Oracle JDeveloper. For information, see the chapter "Integrating the Worklist Service" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

### B.8.1.3 No Rows Yet Message Displays

### Problem

The Worklist task flow continues to display the **No Rows Yet** message.

### Solution

The following are possible solutions to address this problem:

- No **'Assigned'** worklist items exist for the logged in user:



If worklist items are assigned to the logged-in user and the state of these items is **Assigned**, then they always show in the Worklist task flow. The **No Rows Yet** message indicates that no assigned Worklist items exist for the logged-in user. This is not an issue, but expected behavior.

To confirm that this message is displaying correct information, open the Oracle SOA Suite BPEL Worklist application, and check whether any worklist items exist. The URL of BPEL Worklist application is:

`http://host:port/integration/worklistapp`. Where host and port are the same as those used in the Worklist connection.

- The ADF page on which the Worklist task flow exists is not ADF-secured:

The Worklist task flow is not able to query the Worklist repository, because there is no authenticated user associated with the application session to access the Oracle SOA Suite BPEL server. Apply the ADF security on the page. For information, see the section "Setting Security for the Worklist Service in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

## B.8.2 Unavailability of the Worklist Service Due to Server Failure

Server failure is the likely cause of an issue if a Worklist service connection exists, and the Worklist task flow shows the **The Worklist service is unavailable** warning. In case of multiple connections, the **More items not currently available** message displays. These generic warning messages display when there is an issue with Worklist service interactions with the Oracle SOA Suite BPEL repository.

To identify the root cause of the issue, examine the managed server's diagnostic logs at the time when the service fails. In some cases it is necessary to also examine the log files of the managed server on which Oracle SOA Suite BPEL processes are running. Typically, an entry such as the following exists in diagnostic logs of the Worklist application's managed server:

```
[2009-03-23T11:35:21.735+00:00] [DefaultServer] [ERROR]
[WCS-32100] [oracle.webcenter.worklist.model] [tid:
[ACTIVE].ExecuteThread: '0' for queue: 'weblogic.kernel.Default
(self-tuning)'] [userId: user] [ecid:
0000I0n7GBZFk3FLN2o2ye19lrBX00000L,0] [APP: Worklist#V2.0] [arg:
WebCenter Worklist] The WebCenter Worklist has queried the BPEL
Worklist connection named 'WebCenter Worklist', and encountered
a WebCenter Executor error. Please see related exception for
details. If the WebCenter Worklist is running in an Application
Server, check to see if the wsm-pm application is up and
running.
```

This states that there is an issue with the wsm-pm application. There can also be some other causes related to the exception. It is recommended that you examine the logged exceptions when these issues occur.

This section includes the following sub sections:

- [Users Mismatch in Identity Stores](#)
- [Shared User Directory Does Not Include the weblogic User](#)
- [Issues with the wsm-pm Application](#)
- [Clocks are Out of Sync for More Than Five Minutes](#)
- [Worklist Service Timed Out or is Disabled](#)

### B.8.2.1 Users Mismatch in Identity Stores

Mismatch in identity stores used by the managed server on which the Worklist service task flow is running and that of the Oracle SOA Suite BPEL server.

#### Problem

If a user exists in the Worklist managed server's identity store but not in the Oracle SOA Suite's identity store, then the following messages display:

#### In the diagnostic logs of the Worklist service's managed server:

```
[2009-03-23T11:35:21.407+00:00] [DefaultServer] [ERROR] []
[oracle.webcenter.worklist.config] [tid: pool-1-daemon-thread-12] [userId: Luke]
[ecid: 0000I0n7GBZFk3FLN2o2ye19lrBX00000L,0:1:3] [APP: Worklist#V2.0] Error in
workflow service Web service operation invocation.[]
Error in workflow service Web service operation invocation. The error is .
Verify that the SOAP connection information for the server is correct.
ORABPEL-30044
Error in workflow service Web service operation invocation.
Error in workflow service Web service operation invocation. The error is .
Verify that the SOAP connection information for the server is correct.
    at
oracle.bpel.services.workflow.query.client.TaskQueryServiceSOAPClient.convertSOAPF
aultException(TaskQueryServiceSOAPClient.java:242)
    at
oracle.bpel.services.workflow.query.client.TaskQueryServiceSOAPClient.invoke(TaskQ
ueryServiceSOAPClient.java:203)
    at
oracle.bpel.services.workflow.query.client.TaskQueryServiceSOAPClient.authenticate
(TaskQueryServiceSOAPClient.java:253)
    at
oracle.bpel.services.workflow.query.client.AbstractDOMTaskQueryServiceClient.authe
nticate(AbstractDOMTaskQueryServiceClient.java:164)
        at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
        at
sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:39)
        at
sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:
25)
            at java.lang.reflect.Method.invoke(Method.java:597)
            at oracle.webcenter.concurrent.MethodTask.call(MethodTask.java:34)
            at oracle.webcenter.concurrent.Submission$2.run(Submission.java:492)
            at java.security.AccessController.doPrivileged(Native Method)
            at oracle.security.jps.util.JpsSubject.doAsPrivileged(JpsSubject.java:313)
            at oracle.webcenter.concurrent.Submission.runAsPrivileged(Submission.java:499)
            at oracle.webcenter.concurrent.Submission.run(Submission.java:433)
            at
oracle.webcenter.concurrent.Submission$SubmissionFutureTask.run(Submission.java:77
9)
                at java.util.concurrent.Executors$RunnableAdapter.call(Executors.java:441)
                at java.util.concurrent.FutureTask$Sync.innerRun(FutureTask.java:303)
                at java.util.concurrent.FutureTask.run(FutureTask.java:138)
                at
oracle.webcenter.concurrent.ModifiedThreadPoolExecutor$Worker.runTask(ModifiedThre
adPoolExecutor.java:657)
                at
oracle.webcenter.concurrent.ModifiedThreadPoolExecutor$Worker.run(ModifiedThreadPo
olExecutor.java:682)
                    at java.lang.Thread.run(Thread.java:619)
        ]]
[2009-03-23T11:35:21.735+00:00] [DefaultServer] [NOTIFICATION] []
```

```
[oracle.webcenter.worklist.config] [tid: pool-1-daemon-thread-15] [userId: Luke]
[ecid: 0000I0n7GBZFk3FLN2o2ye19lrBX00000L,0:1:6] [APP: Worklist#V2.0]
TaskServiceSOAPClient: soapFault:[[
<env:Fault
xmlns:ns0="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <faultcode>ns0:FailedAuthentication</faultcode>
  <faultstring>FailedAuthentication : The security token cannot be authenticated
or authorized.</faultstring>
  <faultactor/>
</env:Fault>
]]
```

### In the diagnostic logs of the Oracle SOA Suite's managed server:

```
[2009-03-23T04:52:07.909-07:00] [soa_server1] [ERROR]
[WSM-00008] [oracle.wsm.resources.security] [tid:
[ACTIVE].ExecuteThread: '2' for queue: 'weblogic.kernel.Default
(self-tuning)'] [userId: <anonymous>] [ecid:
0000I0nB64fFk3FLN2o2ye19lrBX000000,0:1:3:1] [WEBSERVICE_
PORT.name: TaskQueryServicePortSAML] [APP: soa-infra] [J2EE_
MODULE.name: /integration/services/TaskQueryService]
[WEBSERVICE.name: TaskQueryService] [J2EE_APP.name: soa-infra]
Web service authentication failed.
```

### Solution

The same users must exist in identity stores of both managed servers. For information, see the section "Setting Security for the Worklist Service in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter*.

This can be easily accomplished through the use of a common LDAP identity store. A useful sanity check is to validate that you can log into the Oracle SOA Suite's BPEL Worklist application with the user ID for which the Worklist service is unavailable. That is, try accessing the integration Worklist application at:

`http://host:port/integration/worklistapp`. Where the host and port are the same as those used in the Worklist connection for the task flow application.

## B.8.2.2 Shared User Directory Does Not Include the weblogic User

### Problem

BPEL Web services cannot respond to requests received from the Worklist service because the shared user directory does not include the `weblogic` user.

### Solution

Ensure that you have tried the solution provided in [Users Mismatch in Identity Stores](#). If that solution did not resolve the issue, then try the solution described in this section.

If Oracle SOA Suite is connected to a shared user directory (LDAP), and the user `weblogic` does not exist in the identity store, then the following step assigns the `BPMWorkflowAdmin` role to a valid user in the identity store. Use WLST to revoke an application role from `SOAAdmin` and grant it to a member of the external identity store. This can be done by running the following WLST command from the `ORACLE_HOME`. For example:

```
cd ORACLE_HOME/common/bin/
wlst.sh
connect('weblogic','weblogic', '## soa host ##:## soa administration port ##')
```

```
revokeAppRole(appStripe="soa-infra", appRoleName="BPMWorkflowAdmin",
    principalClass="oracle.security.jps.service.policystore.ApplicationRole",
    principalName="SOAdmin")
grantAppRole(appStripe="soa-infra", appRoleName="BPMWorkflowAdmin",
    principalClass="weblogic.security.principal.WLSUserImpl",
    principalName="user")
```

In this example, the LDAP identity store has a user named `user`. If the user to which you want to grant the `BPMWorkflowAdmin` role does not exist in the LDAP identity store, then you must restart the Oracle SOA Suite's managed server to make this change effective.

### B.8.2.3 Issues with the wsm-pm Application

#### Problem

Issue with the `wsm-pm` application on either the Worklist service's managed server, or the Oracle SOA Suite's managed server, or on both.

#### Solution

The `wsm-pm` application manages the Web service security policies that control the SAML authentication in the Worklist service. To validate this, log into the `wsm-pm` application's validation page as a user with administrative rights. Use this format for validation: `http://host:port/wsm-pm/validator`. If there are no issues with this application, then accessible policies must display. If policies do not display, then investigate the related logged information on the server whose `wsm-pm` application is failing.

### B.8.2.4 Clocks are Out of Sync for More Than Five Minutes

Due to security reasons, the Web service security interaction between the Worklist service's managed server and that of the Oracle SOA Suite BPEL must take place with a time difference of less than five minutes. That is, the clocks on both host machines must have a time difference of less than five minutes, otherwise authentication fails. The SAML assertion uses the `NotBefore` condition to verify this.

#### Problem

Clocks of the Worklist service's managed server and the Oracle SOA Suite BPEL's managed server are out of sync for more than five minutes.

#### Solution

Ensure that the current time is not set to earlier than the SAML assertion's `clockskew`, which is 300 seconds by default.

Either match the time on the client and service machines, or configure the `agent.clock.skew` property (in seconds) in the `policy-accessor-config.xml` file. This file is located in the `DOMAIN_HOME/config/fmwconfig` directory.

### B.8.2.5 Worklist Service Timed Out or is Disabled

#### Problem

The Worklist service is unable to obtain a query result from the Oracle SOA Suite BPEL server within a defined period of time.

The Worklist service issues queries to the Oracle SOA Suite BPEL server using concurrent threads. These threads are allotted a certain amount of time in which to

respond. If these threads do not respond in the allotted time, for example 15 seconds, then the Worklist service times out the call, and it allows the task flow to display the unavailability message. In such a case, log files include related exceptions such as the following:

```
[2009-03-03T12:09:34.769-08:00] [WLS_Spaces] [ERROR] [WCS-32103]
[oracle.webcenter.worklist.model] [tid: [ACTIVE].ExecuteThread: '3' for queue:
'weblogic.kernel.Default (self-tuning)'] [userId: user] [ecid:
0000HzDx68KC0zT6uBbAEH19fOWs00002q,0] [APP: webcenter] Unable to query BPEL
repository.[]
oracle.webcenter.concurrent.TimeoutException: Execution timedout
    queued :      1 ms
    suspended :      0 ms
    running : 15389 ms
    timeout : 15000 ms
    service : Worklist
    resource : ir
    source : oracle.webcenter.concurrent.CallableTask@bf3952
(oracle.webcenter.concurrent.CallableTask)
    submission : 150
    at
oracle.webcenter.concurrent.Submission.transitionTo(Submission.java:595)
    at oracle.webcenter.concurrent.Submission.timeout(Submission.java:634)
    at
oracle.webcenter.concurrent.InternalExecutorService.checkForTimeouts(InternalExecu
torService.java:566)
    at
oracle.webcenter.concurrent.InternalExecutorService.access$300(InternalExecu
torService.java:18)
    at
oracle.webcenter.concurrent.InternalExecutorService$1.run(InternalExecutorService.
java:352)
    at java.util.TimerThread.mainLoop(Timer.java:512)
    at java.util.TimerThread.run(Timer.java:462)]]
```

### Solution

If errors such as this occur consistently, then there may be fundamental issues with the resources available to the managed servers running the Worklist service and the Oracle SOA Suite BPEL server.

Validate that the volume of users and resources provided is adequate to run these servers in the infrastructure provided.

---



---

**Note:** continuous occurrence of `TimeoutExceptions` can also disable the Worklist service. Due to which this service cannot connect to the BPEL instance that is failing to respond in a timely manner. In such a case, the logs contain `oracle.webcenter.concurrent.DisabledException` exceptions. These exceptions are related to the Worklist service failure.

---



---

## B.9 Troubleshooting WebCenter Spaces Import and Export Issues

This section contains the following subsections:

- [ResourceLimitException Issue](#)
- [Page or Group Space Not Found Message After Import](#)

## B.9.1 ResourceLimitException Issue

This section provides the solution to resolve the `ResourceLimitException` issue which occurs during export.

### Problem

In WebCenter Spaces, you try to export all group spaces or entire application and the following error displays:

```
Weblogic.common.resourcepool.ResourceLimitException
```

### Solution

You must increase the maximum capacity in the JDBC connection pool. To do this, log into the WLS Administration Console. From **Services**, select **Data Sources, JDBC**, and then the **Connection Pool** tab.

## B.9.2 Page or Group Space Not Found Message After Import

When users first login to WebCenter Spaces after an import operation they will see a "Page not found" or "Group space not found" if the page or group space they last visited no longer exists. Last accessed page information is retained during import operations which is why the message displays in such instances.

## B.9.3 Group Space Import Exceed Maximum Upload File Size

There is a file size limitation uploading content to WebCenter Spaces. If your export archive exceeds the maximum upload size then the import operation through WebCenter Spaces administration will fail.

Import the group space archive using WLST. See [Section 16.1.9.2, "Importing Group Spaces Using WLST"](#).

Alternatively, modify the content repository upload parameters in `web.xml`. See [Editing web.xml](#).

---

---

# Glossary

## About mode

A **portlet mode** that typically displays information such as copyright, version, and author of the portlet.

## ADF

Application Development Framework. A range of technologies aimed at making **Java EE** application development faster and simpler for developers while at the same time taking advantage of proven software patterns to ensure that the developed application is scalable, performant, and the like.

## administrator

In WebCenter Spaces there are two types of administrator:

- Fusion Middleware administrator: Also referred to as systems administrator. A user with complete administrative capabilities. This administrator can perform the complete range of security-sensitive administrative duties, and all installation, configuration, and audit tasks.
- WebCenter Spaces administrator: A WebCenter Spaces user who is responsible for customizing WebCenter Spaces out of the box, managing and granting application roles, and maintaining the application when it is in use.

## Ajax

A combination of asynchronous JavaScript, dynamic HTML (DHTML), XML, and XMLHttpRequest communication channel that allows requests to be made to the server without fully re-rendering the page. Ajax allows rich client-like applications to use standard internet technologies.

## Announcements service

A WebCenter Web 2.0 service that offers a quick, convenient way to create and widely distribute messages instantly or at a specific time.

## API

Application Programming Interface. A set of exposed data structures and functions that an application can use to invoke services on an application object, such as a **portlet**.

## Application Development Framework

See **ADF**.

**application lifecycle**

The process of creating and testing an application in a design time environment, deploying it to a production system, and then performing routine maintenance, such as monitoring performance and migrating customization data. The lifecycle of an application also includes performing further enhancements, restaging, and then redeploying the application to the production system.

**Application Programming Interface**

See [API](#).

**application role**

Roles that are specific to a particular application and are stored in an application-specific stripe of the policy store.

**application skin**

Specifies the WebCenter Spaces application background color, screen fonts, and, with some skins, the shapes and images used for application buttons and icons. The WebCenter Spaces administrator chooses the default application skin. WebCenter users may change the application skin on the General tab of the Preferences dialog box.

**Applications pane**

An area of the WebCenter Spaces Sidebar that provides convenient access to your frequently used applications.

**authenticated user**

A user who is logged into a [WebCenter application](#). By default, an authenticated user can access public and secured information, such as pages and [portlets](#).

Contrast with [public users](#), who are not logged in, and can access public content only.

**authentication**

Identification of a user through an identity management system. You can require ADF authentication to enforce credentials for users to access the WebCenter application only (all ADF resources in the application remain accessible), or authentication *and* authorization to enforce credentials for users to access the WebCenter application and any ADF resources that have been secured in the application.

**authorization**

The policies that define the access rights of an individual or group to a secured resource. This resource may be a page or component within a page.

**authorized user**

An individual who has access to a secured resource. For non-public resources, this individual is also an [authenticated user](#).

**blog page**

A page that provides a personal record of an individual user's experience and opinions. There are two kinds of blog: personal blogs are written by an individual; group blogs are written by several users.

**Box layout component**

An Oracle Composer layout component. A container that enables the placement of content on a WebCenter Spaces page. In Oracle Composer, a Box is rendered as a



---

rectangle comprised of dashed lines. For designers of custom WebCenter applications, this is the runtime equivalent of a Panel Customizable component.

**BPEL**

Business Process Execution Language. An XML-based markup language for composing a set of discrete Web services into an end-to-end process flow.

**business role page**

A page, created by the WebCenter Spaces administrator, specifically provided for a given role in an organization. Business role pages provide a targeted environment for users of a particular role, by delivering information that is timely and relevant to individual roles without the noise of irrelevant information from other lines of business. Business role pages appear in the personal spaces of users classified under the specified role.

**caching**

The act of storing frequently accessed information, typically Web pages, in a location where it can be accessed quickly to avoid frequent content generation.

See also [expiry-based caching](#) and [validation-based caching](#).

**Change Mode Button component**

A component provided in the Oracle Composer tag library that lets users change from the View mode of a page to Edit mode, in which they can edit the page using Oracle Composer.

**Change Mode Link component**

A component provided in the Oracle Composer tag library that lets users change from the View mode of a page to Edit mode, in which they can edit the page using Oracle Composer.

**check out/check in**

A mechanism that enables a user to lock information, by checking it out, so that other users cannot modify that same piece of information. This prevents users from overwriting each other's changes. After making modifications, the user releases it by checking it back in, making it available again for other users to modify.

**chrome**

Visual elements surrounding a portlet or task flow that provide an access point for actions, such as those on the Actions menu and those embedded in the chrome itself, such as the minimize icon or resize handles.

**Community of Interest group space**

A group space created using the Community of Interest template. This type of group space provides an optimal structure for supporting communities of people, joining together to learn more about a subject area through the sharing of expertise, ideas, and content.

**component**

An individual piece of an application, for example, a task flow, portlet, page, or layout element such as a box or image.

### **Component Catalog**

A dialog, accessed from Oracle Composer, that provides access to all the content you can add to a WebCenter application page.

### **component developer**

The developer who builds components (such as portlets, [JavaServer Faces](#) components, and Web services).

### **Component Properties**

A dialog, accessed from Oracle Composer, that provides access to a component's parameters, display options, style settings, and associated events.

### **container**

An application program or subsystem in which the program building block, known as a component, is run.

### **content integration services**

Services provided by [Oracle WebCenter](#) to enable developers to display content from a [content repository](#), such as by creating [data controls](#).

### **content repository**

A specialized storage and management mechanism, such as author-based versioning, full textual searching, content categorization and attribution, and is optimized for storing unstructured information, which differentiates it from a data repository.

### **content repository data control**

A [data control](#) sourced through a content repository. In a [WebCenter application](#), you can create content repository data controls for the following content repositories: [Oracle Portal](#), [Oracle Universal Content Management](#), and third-party repositories supporting the Java Content Repository (JCR) standard, or your local file system.

### **credential provisioning page**

A [JSF](#) (\* .jspx) page used for authenticating to an [external application](#). At run time, the Credential Provisioning page displays login data fields consisting of the data fields specified through external application registration. Login information is passed to the producer, which in turn passes the login values to the external application. The application provides the producer with the requested portlets.

After authentication, the user's login credentials are preserved in a [credential store](#), which subsequently supplies that information at future sessions. Unless his information changes, the user supplies his credentials only one time.

### **credential store**

A storage area that preserves the login credentials a user provides for authentication to an [external application](#).

### **CSS**

Cascading Style Sheet. A simple mechanism for ensuring a consistent look and feel or adding style, such as fonts, colors, and spacing, to Web documents.

### **custom action**

Icons or menu items that are displayed on the header or in the Actions item of a Show Detail Frame component that surrounds a task flow. These actions can control actions

defined in the task flow itself, enabling task flows to represent internal actions as options on the chrome.

**custom attribute**

Specifies group space information in addition to that provided by the built-in attributes. Custom attributes can be used to determine the content of the components in a group space based on the parameter passed in. For example, a component can display data for a specific customer by passing in the customer ID. A custom attribute is simply a name value pair ; for example customerId=400, orderId=11, userName=Smith, and so on. Custom attributes are stored within the group space template.

**custom page**

Any page created by a user rather than one provided out of the box.

**custom resource catalog**

A resource catalog that has been customized to control the components that are visible to specific users.

Contrast with [default resource catalog](#).

**custom role**

A user role, created by an administrator or a group space moderator, to meet a specific personal space or group space requirement.

**Customize mode**

A [portlet mode](#) that enables users to set the default values for portlet preferences for all users.

**customizable component**

A WebCenter component that can be added to a page at runtime to enable end users to perform personalizations such as move, minimize, restore, or remove on content within those components. Customizable components are the [Panel Customizable component](#) and the [Show Detail Frame component](#).

**customization**

An update that affects all users.

**data control**

A mechanism that provides an abstraction of the business service's data model. The ADF data controls provide a consistent mechanism for clients and Web application controllers to access data objects, collections, methods, and operations.

See also [content repository data control](#).

**default language**

A display language that is used when users log in to WebCenter Spaces. The default language can be overridden temporarily by the session language. The WebCenter Spaces administrator sets the default language on the General tab of the Administration page. Individual users can set their own default language on the General tab of the Preferences dialog box.

**default resource catalog**

The resource catalog that is provided by default for an application. It contains all of the Oracle ADF components and portlets available to the application.

Contrast with [custom resource catalog](#).

### **Default Server**

See [Integrated WLS](#).

### **deployment profile**

A file used in application deployment that specifies the following types of information:

- The source files, deployment descriptors, and other auxiliary files that are packages
- The type and name of the archive file to be created
- Dependency information
- Platform-specific instructions
- Other information

[Oracle WebCenter Services](#) provides a special deployment profile, the [WebCenter application](#) WAR deployment profile, that includes an option to export project metadata.

### **Design view (JDeveloper)**

A view, in [Oracle JDeveloper](#), that provides a WYSIWYG representation of a file.

See also [Source view \(JDeveloper\)](#).

### **Design view (WebCenter Spaces)**

A view, in Oracle Composer, that provides a WYSIWYG representation of a page and its components.

See also [Source view \(WebCenter Spaces\)](#).

### **discoverable group space**

A group space that can be found by anyone logged into WebCenter Spaces, for example through a search. A group space is made discoverable when the group space moderator enables the Discoverable setting. Discoverable group spaces are listed in My Group Spaces; users wishing to join the group space can request membership through self-subscription (if enabled) or by contacting the group space moderator.

### **Discussions service**

A WebCenter Web 2.0 service that provides a means of creating and participating in text-based discussions with members of a particular group space.

### **display language**

Controls the language in which application user interface elements, such as buttons, field labels, and screen text, are rendered in the browser.

### **Document List Viewer task flow**

A Documents service task flow that exposes a list of documents and optionally folders defined by the listing of a specific folder or the results of a document search. Include on a page by selecting All Documents, Group Space Documents, or Personal Documents from the Oracle Composer catalog.

**Documents task flow**

A Documents service task flow that exposes all the folders and files available from the default content repository connection and default folder. Include on a page by selecting Documents from the Oracle Composer catalog. Use to create, upload, and manage library content; to manage file versions; and to check files out and in. Equivalent to Document Library task flow in WebCenter Services Catalog in Oracle WebCenter Framework.

**Documents page**

A predefined page provided in every WebCenter Spaces group and personal space that includes the [Documents task flow](#) for managing content.

**Documents service**

A WebCenter Web 2.0 service that provides features for accessing, adding, and managing files; creating and managing file folders; configuring file and folder properties; and searching file and folder content.

**domain**

Any tree or subtree within the Domain Name System (DNS) namespace. Domain most commonly refers to a group of computers whose host names share a common suffix, the domain name.

**dynamically-generated page**

A page that displays as the result of a user action, such as a search or a click on a tag. As the name suggests, dynamically-generated pages are not stored, but rather are created as and when needed.

**EAR**

Enterprise Archive file. A [Java EE](#) archive file that is used in deploying applications on a [Java EE](#) application server. [WebCenter applications](#) are deployed using both a generic EAR file containing the application and the respective run-time customization and a targeted EAR file containing only the application for deployment to the application server. EAR files simplify application deployment by reducing the possibility of errors when moving an application from development to test, and test to production.

See also [JAR](#) and [WAR](#).

**ECMA-262 specification**

A standardization of scripting programming languages, such as [ECMAScript](#) and [JavaScript](#).

**ECMAScript**

A scripting programming language, standardized by Ecma International according to the [ECMA-262 specification](#). Frequently referred to as [JavaScript](#) or JScript, which are both extensions of the ECMA-262 specification.

**Edit Defaults mode**

([JSR 168](#) portlets only.) A [portlet mode](#) that enables personalization of a JSR 168 portlet. Edit Defaults mode is a display mode for the JSR 168 portlet's properties. In a [WebCenter application](#), the Edit Defaults mode displays on the portlet's Actions menu as the Customize command.

See also [Edit mode](#).

**Edit mode**

A [portlet mode](#) that enables personalization of the portlet for each user, for each instance.

See also [Edit Defaults mode](#).

**edit mode**

A view mode that enables users to modify the content, style, and layout of a page. Access edit mode by choosing Edit Page from the Page Actions menu.

**EL**

Expression Language. Provides a short-hand way of working with Web application data by providing operators for retrieving and manipulating application data residing in a [Java EE](#) Web container. In a [WebCenter application](#), EL expressions are encapsulated in the characters "{" and "}" and typically come in the form #{object.data} where *object* represents any Java object or [ADF](#) component placed in the [Java EE](#) Web container's page, request, session, or application's scope.

**Enterprise Archive file**

See [EAR](#).

**enterprise mashup**

An application that enables users to bring all sorts of content and services together in a single place.

**Events service**

A WebCenter Web 2.0 service that provides group calendars, which you can use to schedule meetings, appointments, and so on. This service is available only in WebCenter Spaces, and not in custom WebCenter applications.

**expiry-based caching**

A [caching](#) method that uses a retention period to specify how long the item is valid in the cache before a refresh is required. When there is a request for the item beyond the retention period, it is refreshed in the cache.

See also [validation-based caching](#).

**Expression Language**

See [EL](#).

**Extensible Markup Language**

See [XML](#).

**external application**

Applications that do not delegate authentication to the single sign-on server. Instead, they display HTML login forms that ask for application user names and passwords. At the first login, users can choose to have the single sign-on server retrieve these credentials for them. Thereafter, they are logged in to these applications transparently.

**farm**

A collection of components managed by Fusion Middleware Control. A farm can contain a Managed Server domain and other Oracle Fusion Middleware system components that are installed, configured, and running on the domain.

**favorites**

A personal list of links to favorite WebCenter Spaces pages and external Web sites.

**Federated Portal Adapter**

See [FPA](#).

**FOD**

Fusion Order Demo. An enterprise application built using Oracle Fusion Middleware, including Oracle WebCenter, used to provide examples of WebCenter functionality.

**FPA**

Federated Portal Adapter. A component of [Oracle Portal](#) that enables Oracle Portal instances to share their database portlets through the Web portlet interface. Using the FPA, Oracle Portal database portlets, including PL/SQL portlets, Portlet Builder portlets, and page portlets can be made available for use in WebCenter applications.

**Full Screen Mode (WebCenter Spaces)**

A view mode that opens the group space to occupy the entire screen, thus maximizing the display space. The Sidebar is not displayed in Full Screen Mode.

**Full Screen mode (Portlets)**

([PDK-Java](#) portlets only.) A [portlet mode](#) that provides more content than can be shown in the portlet when it is sharing a page with other portlets.

**Fusion Middleware Control**

A browser-based management application that is deployed when you install Oracle WebCenter. From Fusion Middleware Control Console, you can monitor and administer a [farm](#) (such as Oracle WebCenter).

**Fusion Order Demo (FOD)**

See [FOD](#).

**Group Project group space**

A group space created using the Group Project template. This type of group space provides an optimal structure for supporting a core project team where each member might come from a different department but all members contribute toward meeting a common goal.

**group space**

A work area within WebCenter Spaces that supports a group of people of any size that is organized around an area of interest or a common goal.

**group space icon**

An image displayed alongside group space names on the Group Spaces page in My Group Spaces to help other users with identification and location.

**group space logo**

An image displayed on the group space Home page to provide a visual identity for the group space. Group space logos also display alongside the group space name at the top of the page in Full Screen Mode.

**group space member**

A user who is participating in a group space. Members can be added or invited to a group space, or they can subscribe to a group space themselves if self-registration is enabled.

**group space owner**

A user who initially created a group space. The group space owner is automatically also a moderator of the group space.

**group space template**

A starting point for group space creation. WebCenter Spaces includes three templates to get you started: Group Project, Community of Interest, and Blank, but you can turn any group space into a template to use it as the starting point for other similar group spaces.

**Group Space Unavailable page**

A predefined page that displays when a group space member tries to open a group space that is temporarily offline. Moderators can customize this page.

**HA**

High Availability. A collection of solutions to ensure that your applications meet the required availability to achieve your business goals, eliminating single points of failure with no or minimal outage in service.

**Help mode**

A [portlet mode](#) that displays usage information about the functionality of the portlet.

**High Availability**

See [HA](#).

**HTML**

Hypertext Markup Language. A format for encoding hypertext documents that may contain text, graphics, and references to programs and other hypertext documents.

**HTML Markup layout component.**

An Oracle Composer layout component. A simple HTML component that renders raw HTML and JavaScript mark-up inline on the page.

**HTTP**

Hypertext Transfer Protocol. The underlying format, or protocol, used across the Web to format and transmit messages and determine what actions [Web servers](#) and browsers should take in response to various commands.

**Hyperlink layout component**

An Oracle Composer layout component. A link to an internal or external Web page. For designers of custom WebCenter applications, this is the runtime equivalent of a Go Link component.

**Hypertext Markup Language**

See [HTML](#).

**Hypertext Transfer Protocol**

See [HTTP](#).



**IDE**

Integrated Development Environment. A visual application development tool containing editors, debuggers, screen painters, object browsers, and the like. [Oracle JDeveloper](#) is an example of an IDE.

**Image layout component**

An Oracle Composer layout component. An illustration that can include a hyperlink. For designers of custom WebCenter applications, this is the runtime equivalent of an Image Link component.

**IMP service**

See [Instant Messaging and Presence service](#).

**initialization parameters**

The parameters initialized upon the start-up of a standard JSR 168 portlet. Initialization parameters provide an alternative to JNDI (Java Naming and Directory Interface) variables. Use initialization parameters instead of JNDI to configure the behavior of all of the different components of the portlet—for example, servlets and other portlets—in a compatible way. In [Oracle WebCenter](#), initialization parameters are entered into the `portlet.xml` file.

**Instant Messaging and Presence service**

A WebCenter Web 2.0 service that enables users to observe the presence status of other authenticated users and provides instant access to interaction options, such as instant messages, emails, and phone calls.

**Integrated Development Environment**

See [IDE](#).

**Integrated WLS**

Integrated WebLogic Server. A WLS instance used as a platform for pretesting WebCenter application deployments on a local computer. Integrated WLS also contains preconfigured portlet producers and several useful prebuilt portlets.

**JAAS**

Java Authentication and Authorization Service (JAAS) is a Java package that enables applications to authenticate and enforce access controls upon users. JAAS is designed to complement Java 2 security and implements a Java version of the standard Pluggable Authentication Module (PAM) framework. This enables an application to remain independent from the authentication service, and supports the use of custom authentication modules.

JAAS extends the access control architecture of the Java 2 Security Model to support subject-based authorization. It also supports declarative security settings, in deployment descriptors, instead of being limited to code-based security settings.

**JAR**

A Java archive file. JAR files contain the class, image, and sound files for a Java application or applet. JAR files may also be compressed.

See also [EAR](#) and [WAR](#).

**Java Authentication and Authorization Service**

See [JAAS](#).

## Java Content Repository

See [JCR 1.0](#).

## Java EE

Also known as Java EE 5. Java Enterprise Edition 5 Platform. A platform that enables application developers to develop, deploy, and manage multitier, server-centric, enterprise-level applications. The Java EE platform offers a multitiered distributed application model, integrated XML-based data interchange, a unified security model, and flexible transaction control. You can build your own Java EE portlets and expose them through Web producers.

## Java Enterprise Edition 5 Platform

See [Java EE](#).

## Java Portlet Specification

Standardizes how components for portal servers are to be developed. This specification defines a common portlet [API](#) and infrastructure that provides facilities for personalization, presentation, and security. Portlets using this [API](#) and adhering to the specification are product-agnostic, and can be deployed to any portal product that conforms to the specification. See also [JSR 168](#).

## Java Specification Request

See [JSR 168](#).

## JavaScript

A scripting language developed by Netscape that enables generation of [portlet](#)s that introduce dynamic behavior in otherwise static HTML. This language is compliant with the European Computer Manufacturing Association's [ECMA-262 specification](#) (ECMA-262 standard). An alternative name for this EMCA-262 language is [ECMAScript](#).

## JavaServer Faces

See [JSF](#).

## JavaServer Page

See [JSP](#).

## JCR 1.0

Java Content Repository 1.0. Also known as JSR 170. It proposes a standard access and interaction [API](#) for content repositories, much like JDBC does for databases.

## JDeveloper

See [Oracle JDeveloper](#).

## JSF

JavaServer Faces. A standard Java framework for building Web applications. It simplifies development by providing a component-centric approach to developing Java Web user interfaces. JSF offers rich and robust [API](#)s that provide programming flexibility and ensures that applications are well designed with greater maintainability by integrating the Model-View-Controller ([MVC](#)) design pattern into its architecture. As JSF is a Java standard developed through Java Community Process, development tools like [Oracle JDeveloper](#) are fully empowered to provide easy to use, visual, and productive development environments for JSF.

## JSF JSP

JavaServer Faces JavaServer Page. JSF JSPs differ from plain JSPs through their support of **Oracle ADF Faces** components for the user interface and JSF technology for page navigation. JSF JSP pages leverage the advantages of the Oracle **Application Development Framework** (Oracle ADF) by using the ADF Model binding capabilities for the components in the pages.

## JSP

JavaServer Page. An extension to servlet functionality that provides a simple programmatic interface to Web pages. JSPs are HTML pages with special tags and embedded Java code that is executed on the Web or application server. JSPs provide dynamic functionality to HTML pages. They are actually compiled into servlets when first requested and run in the servlet container.

See also **JSP tags**.

## JSP tags

Tags that can be embedded in **JSPs** to enclose Java code. These tags use the `<jsp:` syntax and enclose action elements in the JSP with `begin` and `end` tags similar to **XML** elements.

## JSR 168

Java Specification Request (JSR) 168. Defines a set of **APIs** for building standards-based portlets using Java. Portlets built to this specification can be rendered to a portal locally or deployed to a WSRP container for rendering portlets remotely. For more information, see <http://jcp.org/en/jsr/detail?id=168>.

## JSR 170

See **JCR 1.0**

## JSR 301

See **Oracle JSF Portlet Bridge**.

## keystore

A file that provides information about available public and private keys that are used for authentication and data integrity. User certificates and the trust points needed to validate the certificates of peers are also stored securely in the keystore

## layout box

A container that enables placement of content on a WebCenter Spaces page.

## layout component

An object for enhancing the usefulness and appearance of a given page. Layout components include layout boxes, a rich text editor, images, hyperlinks, and so on.

## Layout Customizable component

A component provided in the Oracle Composer tag library that enables users to select from a set of predefined layouts (for example, two column, three column, two row, and so on) and apply it to the page. Users can apply these layouts to a particular area of the page or to the entire page.

## LDAP

Lightweight Directory Access Protocol. A standard, extensible directory access protocol. It is a common language that LDAP clients and servers use to communicate.

The framework of design conventions supporting industry-standard directory products, such as the Oracle Internet Directory.

**lifecycle**

See [application lifecycle](#).

**Lightweight Directory Access Protocol (LDAP)**

See [LDAP](#).

**Links service**

A WebCenter Web 2.0 service that provides a means of creating a bidirectional association between two objects, thus setting up easy access between those objects.

**List Manager**

A task flow of the Lists service that provides access to all the tools for creating and revising lists and list content and to all of a group space's current lists.

**Lists page**

A predefined page that displays the group space's current lists.

**Lists service**

A WebCenter Web 2.0 service for creating, publishing, and managing lists. Uses for lists include tracking issues, capturing project milestones, publishing project assignments, and so on. This service is available only in WebCenter Spaces, and not in custom WebCenter applications.

**Lists Viewer**

A task flow of the Lists service that provides a means of placing a particular list on a group space page.

**Mail service**

A WebCenter Web 2.0 service for exposing familiar mail functionality in WebCenter applications.

**Managed Server**

In a production environment, a Managed Server hosts applications and the resources needed by those applications. A domain, which is a logically related group of Oracle WebLogic Server resources, can have any number of Managed Servers. An Administration Server manages these servers.

**mashup**

A Web application that enables end users to pull information from different sources to create a personalized application that exactly meets their individual requirements.

**MDS**

Oracle Metadata Services. A core technology of the [Application Development Framework](#). MDS provides a unified architecture for defining and using metadata in an extensible and customizable manner.

**Model-View-Controller**

See [MVC](#).

**moderator**

A WebCenter Spaces user who is responsible for managing a particular group space. A group space moderator can add and remove members, invite new members, enable self registration, provide and update group space metadata, and manage the services available to the group space.

**Movable Box layout component**

An Oracle Composer layout component. A container that enables the placement of content on a WebCenter Spaces page and also enables the container (rather than just the content) to be moved around on the page. For designers of custom WebCenter applications, this is the run time equivalent of Show Detail Frame component.

**MVC**

Model-View-Controller. A classic design pattern often used by applications that need the ability to maintain multiple views of the same data. The MVC pattern hinges on a clean separation of objects into one of three categories: models for maintaining data, views for displaying all or a portion of the data, and controllers for handling events that affect the model or views. Because of this separation, multiple views and controllers can interface with the same model. Even new types of views and controllers that never existed before, such as portlets, can interface with a model without forcing a change in the model design.

**My Group Spaces page**

A predefined page that displays a list of all the group spaces and group space templates available to the currently logged in user. This includes group spaces of which the user is a member, group spaces marked as discoverable, and group spaces that are public and available to everyone.

**navigation parameter**

Parameters in a [WSRP](#) container that map to the render parameters with the same name in [JSR 168](#) portlet code. Navigation parameters are exposed by the portlet to the consumer. The consumer stores and manages parameter values and sends them on every invocation to the portlet. Navigation parameters are a WSRP version 2 feature.

**Notes service**

A WebCenter Web 2.0 service that provides useful features for writing personal notes and reminders. This service is available only in WebCenter Spaces, and not in custom WebCenter applications.

**OAM**

See [Oracle Access Manager \(OAM\)](#).

**OHS**

See [Oracle HTTP Server \(OHS\)](#).

**OmniPortlet**

A component of [Oracle WebCenter](#) that enables you to inject portal-like capabilities, such as portlets, content integration, and customization, into your [Oracle ADF Faces](#) applications.

**Oracle Access Manager (OAM)**

Part of Oracle's enterprise class suite of products for identity management and security, Oracle Access Manager provides a wide range of identity administration and

security functions, including several single sign-on options for WebCenter Spaces and WebCenter custom applications. OAM is the recommended single sign-on solution for Oracle WebCenter 11g installations.

**Oracle ADF Faces**

Oracle [ADF Faces](#) is a rich set of user interface components based on the new [JavaServer Faces JSR \(JSR 127\)](#). Oracle ADF Faces provide various user interface components with built-in functionality, such as data tables, hierarchical tables, and color and date pickers, that can be customized and reused in an application.

**Oracle Composer**

A seamlessly integrated environment for populating, revising, and configuring WebCenter application pages. It enables users to easily build or revise page layout and content. It also provides the means of adding different components, such as task flows, portlets, content, and other objects, onto a page and then linking those components for a more relevant or personalized view of the information.

**Oracle Content Server**

Software for building secure business libraries with check in and check out, revision control, and automated publishing in web-ready formats. Current information is available to authorized users anytime, anywhere.

**Oracle Enterprise Manager**

A component that enables administrators to manage Oracle Fusion Middleware services through a single environment. The Fusion Middleware administrator uses Enterprise Manager to configure, manage, and monitor WebCenter applications.

**Oracle HTTP Server (OHS)**

Software that processes Web transactions that use the Hypertext Transfer Protocol (HTTP). Oracle uses HTTP software developed by the Apache Group.

**Oracle Internet Directory**

Oracle's LDAP V3 compliant LDAP server. It is used as the default repository provisioning users and groups. The repository for storing [Oracle Portal](#) user credentials and group memberships. By default, the [Oracle Single Sign-On](#) authenticates user credentials against Oracle Internet Directory information about dispersed users and network resources. Oracle Internet Directory combines LDAP version 3 with the high performance, scalability, robustness, and availability of the Oracle database.

**Oracle JDeveloper**

Oracle JDeveloper is an integrated development environment ([IDE](#)) for building applications and Web services using the latest industry standards for Java, XML, and SQL. Developers can use Oracle JDeveloper to create Java portlets.

**Oracle JSF Portlet Bridge**

Based on and conforming to JSR 301, the Oracle JSF Portlet Bridge enables application developers to expose a JSF application or task flow as a JSR 168 portlet for consumption in another application.

**Oracle Metadata Services**

See [MDS](#).

**Oracle Portal**

A component used for the development, deployment, administration, and configuration of enterprise class [portals](#). Oracle Portal incorporates a portal building framework with self-service publishing features to enable you to create and manage information accessed within your portal.

**Oracle SES**

Oracle Secure Enterprise Search (SES) provides an easy-to-use, Internet-search-like user experience for public and secure sources. Based on crawling agents, the search can include structured and unstructured, public and secure content. Oracle Secure Enterprise Search is included with [Oracle WebCenter](#).

**Oracle Single Sign-On**

A component that enables users to log in to all features of the Oracle Fusion Middleware product suite, and to other Web applications, using a single user name and password.

**Oracle SOA Suite**

A middleware component of Oracle Fusion Middleware. Oracle SOA Suite enables services to be created, managed, and orchestrated into SOA composite applications. Composites enable you to easily assemble multiple technology components into one SOA composite application. Oracle SOA Suite plugs into heterogeneous infrastructures and enables enterprises to incrementally adopt SOA.

**Oracle Technology Network**

See [OTN](#).

**Oracle Universal Content Management**

A consolidated content management application that provides multisite Web content management, document management, digital asset management and records management.

**Oracle WebCenter**

A suite of services that enables you to build custom WebCenter applications. Oracle WebCenter reduces the front-end labor historically required to bring necessary business components to the user by capitalizing on the notion of Service Oriented Architecture (SOA). The suite includes a wide range of plug-and-play products, tools, and services that make it easy to build the applications your users need. Oracle WebCenter includes:

- [Oracle WebCenter Services](#)
- [Oracle WebCenter Framework](#)
- [content integration services](#)
- [ADF](#)
- [Secure Enterprise Search](#)
- Mobile Services
- Portlet Pack

**Oracle WebCenter Framework**

A set of features provided by [Oracle WebCenter](#) that augments the Java Server Faces (JSF) environment by providing additional integration and run-time customization

options It is the basis of Oracle WebCenter and supports the creation and execution of context-rich applications, which can come in the form of human interaction, files and documents, or a clear representation of where the user is within a complex work process. It includes such features as:

- Portlet support
- **content integration services**
- **Oracle JSF Portlet Bridge**
- Search framework
- customizable components

### **Oracle WebCenter Services**

A suite of services included in **Oracle WebCenter** that enables you to enhance your **Oracle ADF Faces** applications with WebCenter application capabilities, such as portlets, content integration, and customization. Includes design time extensions to **Oracle JDeveloper** to help to build **WebCenter applications**. The services include:

- **Oracle Universal Content Management**
- **Secure Enterprise Search**
- communication services

### **Oracle WebLogic Communications Services (OWLCS)**

A comprehensive platform designed to integrate communication services with enterprise services and applications. It includes easy to consume services to support interactions with key communication channels.

### **Oracle WebLogic Server Administration Console**

A browser-based, graphical user interface to manage a WebLogic Server domain. Use to:

- Configure, start, and stop WebLogic Server instances
- Configure WebLogic Server clusters
- Configure WebLogic Server services, such as database connectivity (JDBC) and messaging (JMS)
- Configure security parameters, including creating and managing users, groups, and roles
- Configure and deploy your applications
- Monitor server and application performance
- View server and domain log files
- View application deployment descriptors
- Edit selected run-time application deployment descriptor elements

### **Oracle Wiki and Blog Server**

Provides web services that enable interaction between your application and the wiki.

### **OTN**

Oracle Technology Network. The online Oracle technical community that provides a variety of technical resources for building Oracle-based applications. You can access OTN at <http://www.oracle.com/technology/>.



**OWLCS**

See [Oracle WebLogic Communications Services \(OWLCS\)](#).

**Page Customizable component**

A component provided in the Oracle Composer tag library that defines the editable area of a page at runtime. Within this area, users can edit properties for a component, add content to the page, arrange content, and so on.

**page parameter**

A parameter that enables your page to take values through its URL. Page parameters are defined using the `<parameter>` tag at the top of your `PageDef.xml`. You can bind page parameters to your [page variables](#).

**page parameter**

A parameter associated with a page that can be used to store values that can then be passed to the components on the page

**Page Properties**

A dialog, accessed from Oracle Composer, that provides access to a page's display options, security settings and parameters.

**page scheme**

Determines the background image used in the page. WebCenter Spaces provides several default page schemes and an option for specifying a custom page scheme.

**Page service**

A service for creating new pages and task flows in your application at runtime.

**page style**

Determines the initial page structure, for example one column or two column. Some default page styles also include the task flows, components, and page properties useful for a particular purpose. For example, a page created using the Text page style includes a Text layout component.

**page variable**

A variable that binds your public portlet parameter to the page. Page variables are defined within the `<variableIterator>` of your `PageDef.xml`. One page variable can be bound to multiple public portlet parameters.

**Panel Customizable component**

A component provided in the Oracle Composer tag library that provides a container region for a group of Oracle ADF components and portlets that are customizable at runtime. Any Show Detail Frame components and portlets added as child components to a Panel Customizable component can be moved or maximized with the Panel Customizable component.

**parameter**

A variable that controls the default behavior of task flow content and facilitates the wiring of a task flow to page parameters and page definition variables.

**participant**

A WebCenter Spaces user who can manipulate the content of a group space. A participant can upload and share documents, initiate and take part in chats with other

members, create discussion topics, modify due dates of tasks assigned to them, create new or view existing lists.

**PDK-Java**

Java Portlet Developer Kit. The development framework used to build and integrate Web content and applications with [Oracle WebCenter](#). It includes toolkits, samples, and technical articles that help make portal development simple. You can take existing Java [servlets](#), [JSPs](#), [URL](#)-accessible content and Web services and turn them into [portlets](#). It is typically used by external developers and vendors to create portlets and services.

**personalization**

An update that affects only the user who made it.

**personal page**

A page created by a user in his or her personal space. Personal pages are viewable by other users only if specifically granted access by the user who created the page.

**personal profile**

A page that displays a user's personal information such as email address, phone number, office location, department, manager, direct reports, and so on.

**personal space**

A work area within WebCenter Spaces that provides individual users with a private space for storing personal content, keeping notes, viewing and responding to assignments, maintaining a list of online buddies, and performing many other tasks relevant to their unique working day. Users can also extend this environment by creating additional personal pages and custom content.

**portal**

A common interface (that is, a Web page) that provides a personalized, single point of interaction with Web-based applications and information relevant to individual users or class of users.

**Portal Developer Kit**

See [PDK-Java](#).

**portlet**

A reusable Web component that can draw content from many different sources. Portlets can display excerpts of other Web sites, generate summaries of key information, perform searches, and access assembled collections of information from a variety of data sources. Because different portlets can be placed on a common page, the user receives a single-source experience, even though the content may be derived from multiple sources. Portlet resources include the many prebuilt portlets available out of the box from many sources, programmatic portlets built through WebCenter's JSR 168 and PDK-Java Portlet wizards, and through other portlet building tools.

**portlet mode**

The ways by which a [portlet](#) can be called to display information. These methods include:

- [Shared Screen mode](#) or [View mode](#)
- [Edit mode](#) or [Edit Defaults mode](#)

- [Customize mode](#)
- [Help mode](#)
- [About mode](#)
- [Full Screen mode \(Portlets\)](#) or [Show Details Page mode](#)

### **Portlet Producer Application template**

An application template, provided by JDeveloper, for creating an application with the recommended projects and technology scopes required for developing portlets. The Portlet Producer Application template consists of a single project scoped for portlet creation (Portlets).

See also [WebCenter Application template](#).

### **predefined page**

A page created by WebCenter Spaces to perform a specific function. Examples of predefined pages include, Welcome pages, Search pages and Documents pages.

### **Predeployment Tool**

A utility for [WebCenter applications](#) that helps you configure your target system with the new producer registrations you have added to your application in Oracle JDeveloper. You must run this utility before deploying your application. You can also use this utility after deployment to migrate metadata from stage to production, such as for exporting and importing your customizations. This tool also enables you to define the [MDS](#) repository location to allow run-time customizations to be migrated.

### **pretty URL**

A shortened version of a page's URL that hides the complexity of the real Web address.

### **private parameter**

A portlet parameter that is known only to the portlet itself and has no connection to the page on which the portlet resides.

Contrast with [public parameter](#).

### **producer**

A producer communication link between portlet consumers (such as a [WebCenter application](#) or a [portal](#)). When a consumer application renders a portlet, it calls the producer of that portlet, which in turn executes the portlet and returns the results in the form of portlet content. A producer can contain one or more portlets. A portlet can be contained by only one producer.

[Oracle WebCenter](#) supports two types of producers:

- Oracle [PDK-Java](#) producers: Deployed to a [Java EE](#) application server, which is often remote and communicates through Simple Object Access Protocol (SOAP) over HTTP.
- [Web Services for Remote Portlets](#) (WSRP): A Web services standard that enables the plug-and-play of visual, user-facing Web services with portals or other intermediary Web applications. Being a standard, WSRP enables interoperability between a standards-enabled container based on a particular language (such as [JSR 168](#), .NET, Perl) and any WSRP portal. A portlet (regardless of language) deployed to a WSRP-enabled container can be rendered in any application that supports this standard.

### **programmatic portlets**

Portlets constructed in a non-declarative manner using [APIs](#). Also referred to as *hand-* or *manually coded* portlets.

### **proxy server**

A proxy server typically sits on a network firewall and enables clients behind the firewall to access Web resources. All requests from clients go to the proxy server rather than directly to the destination server. The proxy server forwards the request to the destination server and passes the received information back to the client. The proxy server channels all Web traffic at a site through a single, secure port; this enables an organization to create a secure firewall by preventing Internet access to internal computers, while allowing Web access.

### **public group space**

A group space that is available to all users, even those who are not logged in to WebCenter Spaces.

### **public page**

A page within WebCenter Spaces that is available to all users, even those who are not logged in to WebCenter Spaces.

### **public parameter**

A portlet parameter that is known to the page and bound to it by way of a page variable.

Contrast with [private parameter](#).

### **public user**

A user who can access, but is not logged into, a [WebCenter application](#). A public user can view any page that has been marked as public, but cannot personalize or edit any content, or view pages that have any form of access control.

Contrast with [authenticated user](#).

### **Recent Activities service**

A WebCenter Web 2.0 service that provides a means of tracking recent activities in a WebCenter application.

### **Recent Documents task flow**

A Documents service task flow that exposes the files most recently modified in some way. Include on a page by selecting Recent Documents from the Oracle Composer catalog.

### **resize handle**

A user interface element in a task flow chrome increasing or decreasing the height of the task flow.

### **Resource Action Handling framework**

Enables services that expose custom resources to be viewed, searched, and tagged.

### **Resource Catalog**

A catalog that provides a federated view of one or more otherwise unrelated repositories in a unified search and browse user interface. Resources are created and published in their source repository and are then exposed to the developer in

---

JDeveloper's Resource Palette and to the end user in the Resource Catalog Viewer. Resource catalogs can contain layout components, Oracle ADF components, portlets, service task flows, and documents.

**Reverse Proxy Server**

A server process that hides the physical location of internal servers by exposing the servers as a single public site. Requests to the public site are routed to the appropriate internal server.

**Rich Text portlet**

A portlet, based on the [WSRP](#) standard, offering browser-based rich text editing at run time on a deployed Oracle ADF [JavaServer Faces](#) JSP.

**RSS service**

A WebCenter Web 2.0 service that provides a means of publishing content from other services as news feeds. The RSS service supports both RSS 2.0 and Atom 1.0 formats.

**Search page**

A predefined page for running searches, creating and managing saved searches, and viewing and refining search results.

**Search service**

A WebCenter Web 2.0 service that enables the discovery of information and people in a WebCenter application, returning only the results users are authorized to see

**Secure Enterprise Search**

See [Oracle SES](#).

**secured application page**

A page created by a user that has not been made available to public users.

**Self-Registration page**

A predefined page where users can register with WebCenter Spaces, thus creating themselves an LDAP login account. Administrators can customize certain aspects of this page.

**Self-Subscription page**

A predefined page where users can register to become members of a group space. Moderators can customize certain aspects of this page.

**service ID**

A PDK-Java producer's unique identifier. PDK-Java enables you to deploy multiple producers under a single adapter servlet. Different producers are identified by their unique service IDs. A service ID is required only when a service ID/producer name is not appended to the URL endpoint.

**Service Oriented Architecture**

See [SOA](#).

**servlet**

A Java program that usually runs on a [Web server](#), extending the Web server's functionality. [HTTP](#) servlets take client HTTP requests, generate dynamic content (such as through querying a database), and provide an HTTP response.

### **session language**

A display language specified by the user that remains in effect for the life of the session cookie (usually from the time the user logs on until he logs off). If the user clears browser cookies, the display language reverts to the default language or, if a default language is not specified, the application display language. Set the session language in the Change Language pop-up, accessible from the Welcome page.

### **Shared Screen mode**

A **portlet mode** that renders the body of the portlet and enables you to display a portlet on a page that can contain other portlets. Every portlet must have at least a Shared Screen mode.

See also **View mode**.

### **Show Detail Frame component**

A component provided in the Oracle Composer tag library that renders a border or chrome around the child component. It provides a header with an Actions menu and thereby provides user interface (UI) controls to customize the display of the child component. However, to customize the display of the child component, the Show Detail Frame component must be included inside a Panel Customizable component.

### **Show Details Page mode**

A **portlet mode** that provides full-browser display of the portlet. For example, a portlet in **Show Page mode** could be limited to displaying only the ten most recently submitted expense reports, while the same portlet in Show Details Page mode could show all submissions.

Contrast with **Show Page mode**.

### **show modes**

Types of **portlet modes** encompassing **Show Page mode** and **Show Details Page mode**.

### **Show Page mode**

A **portlet mode** that provides a smaller portlet display to allow space for additional portlets and other objects in the browser window. For example, a portlet in Show Page mode could be limited to displaying only the ten most recently submitted expense reports, while the same portlet in Show Details Page mode could show all submissions.

Contrast with **Show Details Page mode**.

### **Sidebar**

A panel in WebCenter Spaces that provides quick access to tools and information essential to personal productivity, including mail, personal contacts, and so on.

### **skin**

A style sheet based on the CSS 3.0 syntax specified in one place for an entire application. Instead of providing a style sheet for each component, or inserting a style sheet on each page, you can create one skin for the entire application.

### **SOA**

Service Oriented Architecture. A design methodology aimed at maximizing the reuse of application services.

**Source view (JDeveloper)**

A view, in [Oracle JDeveloper](#), that provides a way to directly edit the source code of a file.

**Source view (WebCenter Spaces)**

A view, in Oracle Composer, that provides a selectable structural representation of a page and its components.

See also [Design view \(WebCenter Spaces\)](#).

**struts**

A development framework for Java servlet applications based upon the [MVC](#) design paradigm.

**style properties**

Used to override the style information from the skin CSS to set specific instances of component display.

**Tags service**

A WebCenter Web 2.0 service that enables users to apply their own terms to application objects, making it possible to search for those objects using personally meaningful terms.

**task flow**

A set of ADF Controller activities, control flow rules, and managed beans that interact to allow a user to complete a task. Task flows provide a modular approach for defining control flow in an application. Instead of representing an application as a single JSF page flow, developers can break it up into a collection of reusable task flows.

**task flow header**

An area at the top of a task flow that displays the task flow name and various tools for interacting with the task flow.

**template**

See [group space template](#).

**Text layout component**

An Oracle Composer layout component. A rich text editor for providing static page text. For designers of custom WebCenter applications, this is the runtime equivalent of a Rich Text Editor component.

**Unauthorized Access page**

A predefined page that displays when someone tries to open a page without access permissions. Moderators can customize the default content of this page.

**URL**

Uniform Resource Locator. A compact string representation of the location for a resource that is available through the Internet.

**URL parameter**

See [private parameter](#).

### **validation-based caching**

A [caching](#) method that uses a validation check to determine if the cached item is still valid.

Contrast with [expiry-based caching](#).

### **viewer**

A WebCenter Spaces user who can look at the information in a group space but cannot contribute any of their own.

### **View mode**

([JSR 168](#) portlets only.) A [portlet mode](#) that enables you to display a JSR 168 portlet on a page that can contain other portlets. It is the only required mode for JSR 168 portlets.

See also [Shared Screen mode](#).

### **WAR**

Web application archive file. This file is used in deploying applications on a [Java EE](#) application server. WAR files encapsulate in a single module all of the components necessary to run an application. WAR files typically contain an application's [servlet](#), [JSP](#), and [JSF JSP](#) components.

See also [EAR](#) and [JAR](#).

### **Web 2.0**

Technologies, such as wiki, RSS, and blogs, that enable the construction of highly interactive Web applications.

See also [WebCenter Web 2.0 service](#).

### **Web Application Archive file**

See [WAR](#).

### **Web clipping**

A feature that enables page designers to collect Web content into a single centralized portal. It can be used to consolidate content from hundreds of different Web sites scattered throughout a large organization.

### **Web Clipping portlet**

A browser-based declarative tool that enables you to integrate any Web application with your [WebCenter application](#). It is designed to give you quick integration by leveraging the Web application's existing user interface. You can drag and drop Web Clipping portlets on to a \*.jspx page.

### **Web Page layout component**

An Oracle Composer layout component. A means of embedding another Web site, wiki, or blog within the context of a WebCenter Spaces page. For designers of custom WebCenter applications, this is the equivalent of an Inline Frame component.

### **Web server**

A program that delivers Web pages.

### **Web Services for Remote Portlets**

See [WSRP](#).



**WebCenter**

See [Oracle WebCenter](#).

**WebCenter application**

An ADF application that combines Web content, portlets, and collaborative services for the end user. Administrators can customize the [WebCenter application](#) based on their roles and skill levels in the organization.

**WebCenter application administrator**

The administrator responsible for maintaining the [WebCenter application](#). This administrator performs tasks such as implementing the branding for the WebCenter application, making new content available, modifying pages, and granting and revoking privileges.

Contrast with Fusion Middleware Administrator who is responsible for setting up and configuring WebCenter Spaces, and performing on-going administrative tasks for WebCenter Spaces and other WebCenter components.

**WebCenter application developer**

The developer who plans, builds, and maintains a [WebCenter application](#) using the Oracle Application Development Framework, [Oracle JDeveloper](#), and the [Oracle WebCenter](#).

**WebCenter application end user**

The WebCenter application end user is the run time user of the [WebCenter application](#), who accesses pages, portlets, and content, and personalizes portlets (assuming the appropriate privileges).

**WebCenter Application template**

An application template, provided by JDeveloper, for creating an application with the recommended projects and technology scopes required for developing a WebCenter application. The WebCenter Application template consists of a project for the data model (Model) and a project for consuming portlets, components, and data controllers (ViewController).

See also [Portlet Producer Application template](#).

**WebCenter Extension for Oracle JDeveloper**

An extension available through the Oracle JDeveloper Update Wizard that installs the necessary libraries, templates, wizards, and dialogs needed to build and deploy [WebCenter applications](#) in [Oracle JDeveloper](#).

**WebCenter Framework**

See [Oracle WebCenter Framework](#).

**WebCenter Services**

See [Oracle WebCenter Services](#).

**WebCenter Spaces**

A Web-based application that offers the very latest technology for social networking, communication, collaboration, and personal productivity. WebCenter Spaces uses services and applications to bring everything together that users require to exchange ideas with others, keep track of personal and work-related tasks, interact with critical

applications, and zero in on projects and interests; all within a single integrated environment.

### **WebCenter Spaces application administrator**

See [administrator](#).

### **WebCenter Spaces RSS reader**

An RSS reader provided with WebCenter Spaces that incorporates public news feeds from external sources onto application pages. This RSS reader is available only in WebCenter Spaces, and not in custom WebCenter applications.

### **WebCenter systems administrator**

See [administrator](#).

### **WebCenter Web 2.0 service**

A service that provides Web 2.0 functionality in support of personal and team objectives. WebCenter provides the following services:

- [Announcements service](#)
- [Discussions service](#)
- [Documents service](#)
- [Events service](#)
- [Instant Messaging and Presence service](#)
- [Links service](#)
- [Lists service](#)
- [Mail service](#)
- [Notes service](#)
- [Recent Activities service](#)
- [RSS service](#)
- [Search service](#)
- [Tags service](#)
- [Worklist service](#)

### **WebLogic Server**

See [WLS](#).

### **Welcome page**

There are two types of Welcome page:

- **Public Welcome page:** A predefined page that users encounter before logging in to WebCenter Spaces.
- **Personal Welcome page:** A predefined page that introduces users to their personal space.

### **wiki page**

A page that provides in-place editing using HTML or a simple mark-up language. Any user with sufficient privileges can add, revise, and remove information.

**WLS**

WebLogic Server. A scalable, enterprise-ready Java Platform, Enterprise Edition (Java EE) application server. The WebLogic Server infrastructure supports the deployment of many types of distributed applications and is an ideal foundation for building applications based on Service Oriented Architectures (SOA).

See also [Integrated WLS](#)

**WLST**

WebLogic Scripting Tool. A command line tool for managing Oracle Fusion Middleware components, such as Oracle WebCenter.

**Worklist service**

A WebCenter Web 2.0 service that provides access to notifications, alerts, and BPEL tasks assigned to the current user.

**WSRP**

Web Services for Remote Portlets (WSRP) is a Web services standard that allows the plug-and-play of visual, user-facing Web services with portals or other intermediary Web applications. Being a standard, WSRP enables interoperability between a standards-enabled container based on a particular language (such as [JSR 168](#), .NET, Perl) and any WSRP portal. A portlet (regardless of language) deployed to a WSRP-enabled container can be rendered on any portal that supports this standard.

**XML**

Extensible Markup Language (XML) is an open standard for describing data using a subset of the SGML syntax.

**XSL**

Extensible Stylesheet Language (XSL) is the language used within style sheets to transform or render [XML](#) documents.



---

---

# Index

## A

---

- access protocols, 1-6
- addWorklistConnection (WLST Command), 11-49
- ADF Client State Token, A-9
- ADF Faces skins (WebCenter Spaces)
  - creating, 18-7
  - default, 18-6
  - selecting, 18-7
  - using, 18-6
- ADF libraries, 1-5, 1-6
- ADF security
  - about, 14-3
  - permission-based authorization, 14-6
  - role-mapping based authorization, 14-6
- adf-config.xml, 1-7
- Admin role (WebLogic Server), 1-10
- Administration link (WebCenter Spaces), 17-1
- Administration pages (WebCenter Spaces), 17-1
  - General page, 17-3
  - Group Spaces page, 17-3
  - Personal Space page, 17-3
  - Security page, 17-3
  - Services page, 17-3
  - Welcome page, 17-3
- administration server
  - Administration Console, 1-13
  - out-of-the-box, 1-4
- administration tools
  - Fusion Middleware Control, 1-13
  - WebCenter Spaces Administration pages, 1-16
  - WebLogic Scripting Tool (WLST), 1-14
  - WebLogic Server Administration Console, 1-13
- Administrator role (WebCenter Spaces), 19-2
  - assigning a user, 19-10
  - logging in, 17-1
- Announcements service, A-12, A-14
  - connection
    - activating, 11-7
    - creating, 11-4
    - deleting, 11-10
    - managing, 11-2
    - modifying, 11-9
  - performance issues and actions, 15-37
  - performance metrics, 15-9
  - root category, 18-11

- anonymous access on wiki and blog server, 11-68
- anonymous-role, 19-2
- Application Developer Framework, 1-3
- application permissions (WebCenter Spaces), 19-3
- application roles (WebCenter Spaces), 19-2
  - assigning users, 19-7
  - changing users, 19-8
  - creating, 19-12
  - custom, 19-3
  - default roles, 19-2
  - deleting, 19-15
  - granting permissions, 19-13
  - permissions, 19-3
  - revoking from a user, 19-10
- application skins (WebCenter Spaces)
  - creating, 18-7
  - default, 18-6
  - using, 18-6
- application templates (WebCenter Spaces), 18-18
- Applications pane (WebCenter Spaces), 21-1
  - arranging applications, 21-6
  - editing links, 21-5
  - locking applications, 21-7
  - making applications available, 21-2
  - removing links, 21-8
- Application-View permission, 18-17
  - granting to Public-User role, 19-14
- authenticated-role, 19-2
- Authentication Method, 13-6
- automatic login (external applications), 13-4

## B

---

- backup and recovery
  - about, 16-41
  - Oracle WebCenter Wiki and Blog Server, 11-73
  - WebCenter Web 2.0 Services back-end
    - components, 16-41
- BASIC Authentication Method, 13-6
- blog entries, deleting, 11-70
- Blog service, configuration, 11-53
- BPEL servers
  - configuring WebCenter Spaces workflows, 9-1
  - configuring WS-Security, 14-168
  - hosting WebCenter Spaces workflows, 9-1
  - LDAP identity store, 11-44

- managing connections, 11-43
- performance issues and actions, 15-37
- performance metrics, 15-10
- prerequisites, 11-44
- registering, 11-45
- single sign-on, 11-45
- WS-Security, 11-45
- branding WebCenter Spaces, 18-1
- browser language (WebCenter Spaces), 18-8
- business role pages (WebCenter Spaces), 20-1
  - copying, 20-8
  - creating, 20-2
  - deleting, 20-9
  - display order, 20-6
  - editing, 20-7
  - restricting public access, 20-21
  - target audience, 20-3

## C

---

- Change Center, 1-14
- checklists
  - administering custom WebCenter applications, 5-1
  - administering WebCenter Spaces, 3-1
  - getting custom WebCenter applications up and running, 4-1
  - getting WebCenter Spaces up and running, 2-1
- chrome, 18-18
- CLIENT\_STATE\_MAX\_TOKENS, A-9
- cluster configuration, A-5
- command-line configuration (WLST), 1-14
- composite applications, 1-4
- Concurrency Management, A-10
- configuration files
  - adf-config.xml, 1-7, A-1
  - connections.xml, 1-7, A-1
  - editing manually, A-6
  - handling conflicts, A-3
  - web.xml, A-1
- connections
  - configuring the WebCenter repository, 11-51
  - deployed applications
    - setting up Discussions and Announcements, 11-2
    - setting up Instant Messaging and Presence, 11-12
    - setting up Mail, 11-26
    - setting up Search, 11-36
    - setting up wikis and blogs, 11-53
    - setting up Worklists, 11-43
  - managing post deployment
    - custom WebCenter applications, 6-6
    - WebCenter Spaces, 6-3
  - sconfiguring MDS repository, 11-53
- connections.xml, 1-7
- content repositories
  - about connections, 10-2
  - active connection, 10-2, 10-16
  - changing active connection using Fusion Middleware Control, 10-16
  - changing active connection using WLST, 10-17
  - connection information files, 10-2
  - default connection, 10-2, 10-16
  - deleting connections using Fusion Middleware Control, 10-18
  - deleting connections using WLST, 10-19
  - file system, 10-10
  - managing, 10-1 to ??
  - managing connection properties (WebCenter Spaces) using Fusion Middleware Control, 10-19
  - managing connection properties (WebCenter Spaces) using WLST, 10-20
  - modifying connection details using Fusion Middleware Control, 10-17
  - modifying connection details using WLST, 10-18
  - Oracle Content Server, 10-3
  - Oracle Portal, 10-9
  - performance metrics, 15-10
  - prerequisites, 10-3
  - registering using Fusion Middleware Control, 10-10
  - registering using WLST, 10-15
- copyright statement (WebCenter Spaces), 18-7
- createBPELConnection (WLST command), 11-48
- createDiscussionForumConnection (WLST Command), 11-7
- createExtAppConnection (WLST Command), 13-7
- createIMPConnection (WLST command), 11-22
- createJCRContentServerConnection (WLST command), 10-15
- createJCRFileSystemConnection (WLST command), 10-15
- createJCRPortalConnection (WLST command), 10-15
- createMailConnection (WLST command), 11-32
- createSESSConnection (WLST command), 11-40
- credential provisioning, 13-1
  - public credentials, 13-7
  - shared credentials, 13-7
- CRUD APIs, A-11
- custom application roles (WebCenter Spaces), 19-3
- custom managed servers, 1-5
- custom WebCenter applications
  - about, 1-9
  - administering applications (checklist), 5-1
  - deploying, 7-1, 7-18
  - export and import, 16-34
  - getting applications up and running (checklist), 4-1
  - home page in Fusion Middleware Control, 6-5
  - monitoring performance, 15-43
  - starting and restarting
    - using Fusion Middleware Control, 8-5
    - using WLST, 8-5
  - stopping
    - using Fusion Middleware Control, 8-6
    - using WLST, 8-6
  - undeploying, 7-29
  - viewing and configuring logs, 15-44

customizations in MDS, A-2

## D

---

database connection, changing (WebCenter repository), 11-53

deleteConnection (WLST command), 10-19, 11-11, 11-26, 11-35, 11-43, 11-51, 13-9

deleteDocumentsSpacesProperties (WLST command), 10-20

deployment

- custom WebCenter applications, 7-1, 7-18
- EAR file, 7-2
- portlet producer applications, 1-12, 7-1
- understanding, 7-2
- using Fusion Middleware Control, 7-19
- using JDeveloper, 7-19
- using WLS Administration Console, 7-26
- using WLST, 7-24
- WebCenter applications, 1-12
- WebCenter Spaces, 1-12
- WebLogic Managed Server, creating, 7-2
- WebLogic Managed Server, provisioning, 7-2

deregisterOOTBProducers (WLST Command), 12-13

deregisterPDKJavaProducer (WLST Command), 12-13

deregisterSampleProducers (WLST Command), 12-13

deregisterWSRPProducer (WLST command), 12-13

diagnostic log files, 1-9

discussion forums (WebCenter Spaces), 19-3

- publishing group space mail, 18-12
- root category on server, 18-11
- specifying group space default, 18-12

Discussions server

- configuration files
- exporting, 16-12
- exporting for group spaces, 16-23
- importing, 16-12
- importing for group spaces, 16-25
- LDAP identity store, 11-3, 14-35, 14-36
- managing connections, 11-2
- performance metrics, 15-9, 15-15
- prerequisites, 11-2
- registering, 11-4
- role mapping (WebCenter Spaces), 19-5
- WS-Security, 11-3, 14-176

Discussions servers

- configuring WS-Security, 14-176

Discussions service, A-12

connection

- activating, 11-7
- creating, 11-4
- deleting, 11-10
- managing, 11-2
- modifying, 11-9

performance issues and actions, 15-37

performance metrics, 15-15

root category, 18-11

troubleshooting, B-7

display language (WebCenter Spaces), 18-8

distribution lists (group spaces), 18-12, B-10

Documents service

- content repositories, 10-2
- exporting group space content, 16-29
- importing group space documents, 16-29
- performance issues and actions, 15-37
- performance metrics, 15-10

domain (wc\_domain), 1-4

domains (wiki)

- creating domains, 11-59
- editing domain menu, 11-60
- managing domain members, 11-62

## E

---

EAR files

- deploying, 7-2

Enterprise Manager

*See also* Fusion Middleware Control

export and import

- about, 16-1

- about group space templates, 16-3

- about group spaces, 16-3

- custom WebCenter applications, 16-34

- exporting data, 16-39

- exporting portlet client metadata, 16-35

- exporting WebCenter Web 2.0 Services

- metadata and data, 16-36

- importing data, 16-40

- importing portlet client metadata, 16-35

- importing WebCenter Web 2.0 Services

- metadata and data, 16-38

- migrating application security policies, 16-39

- migrating data, 16-39

- prerequisites, 16-34

- exporting group space templates from WebCenter Spaces, 16-32

- exporting group space templates using WLST, 16-32

- exporting group spaces from WebCenter Spaces, 16-31

- exporting group spaces using WLST, 16-31

- group space templates, 23-1

- group spaces, 23-1

- back-end components, 16-22

- exporting discussions, 16-23

- exporting documents, 16-29

- exporting wikis and blogs, 16-27

- importing discussions, 16-25

- importing documents, 16-29

- importing wikis and blogs, 16-28

- importing group space templates from WebCenter Spaces, 16-33

- importing group space templates using WLST, 16-33

- importing group spaces from WebCenter Spaces, 16-32

- importing group spaces using WLST, 16-32

- migrating group space templates

- back-end component, 16-32
- migration tools, 16-34
- prerequisites for group spaces, 16-22
- WebCenter Spaces
  - about, 16-1, 16-2
  - back-end components, 16-6
  - credential store, 16-8
  - customizations and personalizations, 16-3
  - exporting discussions server, 16-12
  - exporting entire producer metadata, 16-16
  - exporting LDAP identity store, 16-7
  - exporting Oracle Content Server, 16-15
  - exporting Oracle WebCenter Wiki and Blog Server, 16-13
  - exporting Oracle WebLogic Communications Server, 16-16
  - exporting using Fusion Middleware Control, 16-17
  - exporting using WLST, 16-20
  - importing discussions server, 16-12
  - importing entire producer metadata, 16-17
  - importing LDAP identity store, 16-7
  - importing Oracle Content Server, 16-15
  - importing Oracle WebCenter Wiki and Blog Server, 16-14
  - importing Oracle WebLogic Communications Server, 16-16
  - importing using Fusion Middleware Control, 16-21
  - importing using WLST, 16-22
  - policy store, 16-10
  - prerequisites, 16-6
  - recommendations for import, 16-20
  - troubleshooting, B-20
- exportMetadata, A-3
- external applications
  - about, 13-1
  - additional login fields, 13-6
  - deleting using Fusion Middleware Control, 13-9
  - deleting using WLST, 13-9
  - launching from WebCenter Spaces sidebar, 21-2
  - managing post deployment
    - custom WebCenter applications, 6-6
    - WebCenter Spaces, 6-3
  - modifying using Fusion Middleware Control, 13-8
  - modifying using WLST, 13-8
  - performance issues and actions, 15-38
  - performance metrics, 15-19
  - registering using Fusion Middleware Control, 13-3
  - registering using WLST, 13-7

## F

---

- file size, changing upload maximum, 10-24
- file system
  - connection parameters, 10-15
  - content repository prerequisites, 10-10
  - limitations in WebCenter, 10-10

- security considerations, 10-10
- files, maximum upload size, 10-24
- Fusion Middleware administrators, 3-1
  - Admin role, 1-10
  - Monitor role, 1-10
  - Operator role, 1-10
  - roles and responsibilities (custom WebCenter applications), 4-1, 5-1
  - roles and responsibilities (WebCenter Spaces), 2-1
- Fusion Middleware Control
  - about, 1-13
  - changing content repository active connection, 10-16
  - custom WebCenter application home page, 6-5
  - deleting content repository connections, 10-18
  - deleting producer connections, 12-13
  - deploying custom WebCenter applications, 7-19
  - deploying portlet producer applications, 12-15
  - editing producer connection details, 12-11
  - exporting WebCenter Spaces, 16-17
  - importing WebCenter Spaces, 16-21
  - managed server, creating, 7-8
  - managing Announcements service connections, 11-2
  - managing content repository connection properties (WebCenter Spaces), 10-19
  - managing Discussions service connections, 11-2
  - managing Instant Messaging and Presence service connections, 11-12
  - managing Mail service connections, 11-26
  - managing Search service connections, 11-36
  - managing Worklist service connections, 11-43
  - modifying content repository connection details, 10-17
  - monitoring WebCenter applications, 15-1
  - operation summary, 1-11
  - redeploying custom WebCenter applications, 7-33
  - redeploying portlet producer applications, 7-33
  - registering an MDS schema, 7-15
  - registering content repositories, 10-10
  - registering Oracle PDK-Java producers, 12-8
  - registering WSRP producers, 12-2
  - starting, 6-1
  - undeploying custom WebCenter applications, 7-29
  - undeploying portlet producer applications, 7-29
  - WebCenter Spaces home page, 6-2

## G

---

- garbage collector, A-7
- GET Authentication Method, 13-6
- getRSSProxyConfig (WLST command), 11-73
- Global Help URL
  - online help link (WebCenter Spaces), 18-2
- Group Space Events service
  - managing connection, 11-51, 11-53
  - performance issues and actions, 15-38



- performance metrics, 15-17
- group space templates
  - about export and import, 16-3
  - deleting, 22-8
  - export and import
    - back-end components, 16-32
    - exporting from WebCenter Spaces, 16-32
    - exporting using WLST, 16-32
    - importing from WebCenter Spaces, 16-33
    - importing using WLST, 16-33
  - exporting, 23-6
  - importing, 23-7
  - managing, 22-7
  - publishing and unpublishing, 22-9
  - viewing, 22-7
- group spaces
  - about import and export, 16-3
  - bringing online, 22-3
  - changing status, 22-2
  - closing, 22-4
  - default discussion forums, 18-12
  - deleting, 22-6
  - enabling and disabling services, 18-17, 22-6
  - export and import
    - back-end components, 16-22
    - exporting discussions, 16-23
    - exporting documents, 16-29
    - exporting from WebCenter Spaces, 16-31
    - exporting using WLST, 16-31
    - exporting wikis and blogs, 16-27
    - importing discussions, 16-25
    - importing documents, 16-29
    - importing from WebCenter Spaces, 16-32
    - importing using WLST, 16-32
    - importing wikis and blogs, 16-28
    - prerequisites, 16-22
  - exporting, 23-1
  - importing, 23-4
  - managing, 22-1
  - performance metrics, 15-40
  - permissions, 19-3
  - publishing group mail, 18-12
  - reactivating, 22-5
  - resource catalog customization, 18-20
  - subscription workflows, 9-1
  - taking offline, 22-3
  - templates
    - deleting, 22-8
    - managing, 22-7
    - publishing and unpublishing, 22-9
    - viewing, 22-7
  - templates permissions, 19-3
  - viewing information, 22-2

## H

---

- heap size, A-7
- Help link (WebCenter Spaces), 18-2
- HTTP Session Timeout, A-8

## I

---

- identity store, personal profile data (WebCenter Spaces), 18-13
- IMAP, 11-26
  - SSL security, 11-28
- import and export
  - group space templates, 23-1
  - group spaces, 23-1
  - performance issues and actions, 15-38
  - performance metrics, 15-22
- installation, 1-10
- Instant Messaging and Presence service, A-13
  - connection
    - activating, 11-22
    - creating, 11-22
    - deleting, 11-25
    - managing, 11-12
    - modifying, 11-24
  - performance issues and actions, 15-38
  - performance metrics, 15-21
  - troubleshooting, B-8

## J

---

- J2EE application
  - home page in Fusion Middleware Control, 6-5
- Java Keystore, 14-186
- JDBC data source, A-6
- JDeveloper
  - deploying custom WebCenter applications, 7-19
- JNDI Name, 11-53
- JRF libraries, 1-6
- JRockit, A-6
- JSP Page Timeout, A-9
- JVM arguments, A-6, A-7
- JVM\_ARGS, 1-15

## K

---

- keystores for WSRP producers, 14-185

## L

---

- language support (WebCenter Spaces), 18-8
- LCS
  - See* Microsoft Live Communications Server, 11-12
- LDAP identity store
  - about, 14-5
  - adding users, 14-18
  - BPEL server requirements, 11-44
  - Discussions server requirements, 11-3
  - exporting, 16-7
  - exporting and importing credential store, 16-8
  - exporting and importing policy store, 16-10
  - external LDAP, 14-9
    - moving admin account, 14-26
  - importing, 16-7
  - LCS server requirements, 11-17
  - OWLCS server requirements, 11-13
  - reassociating, 14-10

- tuning, 14-17
- LDIF files
  - adding users to LDAP, 14-22
  - creating, 14-23
  - root node, 14-37
- Links service
  - managing connection, 11-51, 11-53
  - permissions (WebCenter Spaces), 19-3
- listDocumentsSpacesProperties (WLST command), 10-20
- Lists service
  - managing connection, 11-51, 11-53
  - performance issues and actions, 15-38
  - performance metrics, 15-22
- Lock and Edit (WebLogic Administration Console), 1-14
- log files, 1-9
- Login page (WebCenter Spaces)
  - customizing default, 20-18
  - default, 20-19
- logo (WebCenter Spaces), 18-5
- Logout link, wiki and blog server, 11-54
- logs
  - configuring, 15-44
  - custom WebCenter applications, 15-44, 15-45
  - viewing, 15-44
  - WebCenter Spaces, 15-44

## M

---

- mail servers
  - managing connections, 11-26
  - performance metrics, 15-24
  - prerequisites, 11-27
  - registering, 11-28
- Mail service, A-13
  - connection
    - activating, 11-32
    - creating, 11-28
    - deleting, 11-35
    - managing, 11-26
    - modifying, 11-34
  - performance issues and actions, 15-38
  - performance metrics, 15-24
  - troubleshooting, B-9
- managed server
  - creating, 7-2
  - creating using Jython script, 7-9
  - provisioning, 7-2
- managed server, creating using Fusion Middleware Control, 7-8
- managed server, creating using WLS Administration Console, 7-3
- managed servers
  - out-of-the-box, 1-4
  - SOA, 9-1
  - start up order, 1-6
  - starting and stopping, 8-2
  - WLS\_Portlets, 1-5
  - WLS\_Services, 1-5

- WLS\_Spaces, 1-5
- MDS (Metadata Service) repository
  - creating, 7-11
  - registering, 7-11
- MDS Cache Size, A-9
- MDS customizations, 1-7
- MDS Purge Rate, A-9
- MDS repository
  - application startup failure
  - base file locations, A-2
  - configuration files, 1-7
  - configuring, 11-53
  - customizations, A-2
- MDS schema
  - creating, 7-11
  - registering, 7-11
  - registering using Fusion Middleware Control, 7-15
  - registering using WLST, 7-17
- menu (wiki)
  - about domain menu, 11-60
  - editing domain menu, 11-61
- Metadata Service (MDS) repository
  - creating, 7-11
  - registering, 7-11
- Microsoft Exchange Server
  - registering, 11-28
  - setting up mail connections, 11-26
- Microsoft Live Communications Server
  - LDAP identity store, 11-17
  - performance metrics, 15-21
  - prerequisites, 11-13
  - registering, 11-18
  - setting up connections, 11-12
  - SSL security, 14-71
- Monitor role (WebLogic Server), 1-10
- monitoring
  - Oracle WebCenter Wiki and Blog Server, 11-72
  - WebCenter applications, 15-1
  - WebCenter Spaces, 15-1
- monitoring performance
  - common performance issues and actions, 15-7
  - custom WebCenter applications, 15-43
  - metrics common across WebCenter services, 15-3
  - recent history and since startup, 15-2
  - WebCenter Spaces, 15-42

## N

---

- Node Manager, 8-2
- Notes service
  - managing connection, 11-51, 11-53
  - performance issues and actions, 15-39
  - performance metrics, 15-26

## O

---

- OAM-SSO, B-8
- OmniPortlet, A-15
- open-files-limit, A-6

- Operator role (WebLogic Server), 1-10
- Oracle Access Manager
  - Access Server, 14-74
  - components, 14-73
  - configuring, 14-72
  - configuring using scripts, 14-74
  - Identity Assertion Provider, 14-74
  - logout from SSO applications, 14-3
  - single sign-on, 14-9
  - WebGate, 14-74
- Oracle Application Server Single Sign-On, 14-100
  - components, 14-101
- Oracle Content Server
  - configuration, 10-3
  - configuring identity store, 10-3, 14-37
  - configuring SSL, 10-5
  - connection parameters, 10-13
  - content repository prerequisites, 10-3
  - enabling full-text search and indexing, 10-5
  - exporting, 16-15
  - exporting for group spaces, 16-29
  - importing, 16-15
  - importing group space documents, 16-29
  - installation, 10-3
  - security considerations, 10-8
  - verifying signatures, 10-7
  - WebDAV URL, 18-17
- Oracle DMS, 1-6
- Oracle Enterprise Manager
  - See also* Fusion Middleware Control
- Oracle Internet Directory, 14-5, 14-9, 14-11, 14-24, 14-41, 14-68
- Oracle Metadata Repository
  - See* MDS repository
- Oracle PDK-Java producers, 12-8
- Oracle Platform Security Services, 14-3, 14-6
  - APIs, 14-9
- Oracle Portal
  - configuration, 10-9
  - connection parameters, 10-14
  - content repository prerequisites, 10-9
  - installation, 10-9
  - limitations in WebCenter, 10-9
- Oracle Secure Enterprise Search
  - See* Secure Enterprise Search, 11-36
- Oracle SOA Suite, 9-1
- Oracle Web Services Manager (wsm-pm), 1-6
- Oracle WebCenter
  - about, 1-1
  - ADF security, 14-1
  - administration tools, 1-12
  - administrative roles, 1-10
  - architecture, 1-2
  - configuration files, A-1
  - configuration overview, 1-7
  - configuration tools, A-5
  - default security, 14-4
  - deployment, 1-12
  - external dependencies, 1-6
  - installation, 1-10
  - log files, 1-9
  - managed servers, 1-5
  - performance monitoring, 1-12
  - topology, 1-4
- Oracle WebCenter Discussions Server
  - See* Discussions server
- Oracle WebCenter Spaces
  - See* WebCenter Spaces
- Oracle WebCenter Wiki and Blog Server
  - accessing the server, 11-58
  - Administration mode
    - accessing, 11-55
    - features, 11-56
  - anonymous access, 11-68
  - backing up, 11-73
  - blocking an IP address, 11-69
  - configuration files, 1-8
  - configuring features, 11-72
  - configuring parameters, 11-70
  - configuring wiki repository, 11-71
  - exporting, 16-13
  - exporting for group spaces, 16-27
  - importing, 16-14
  - importing for group spaces, 16-28
  - Logout link, 11-54
  - monitoring, 11-72
  - permissions, 11-67
  - prerequisites, 11-53
  - testing server connection, 11-58
  - troubleshooting, B-12
- Oracle WebLogic Communications Server
  - configuring WS-Security, 14-178
  - exporting, 16-16
  - importing, 16-16
  - LDAP identity store, 11-13
  - performance metrics, 15-21
  - prerequisites, 11-13
  - registering, 11-18
  - setting up connections, 11-12
  - SSL security, 11-14, 14-70
  - WS-Security, 11-14
- Oracle WebLogic Scripting Tool
  - about, 1-14
  - running, 1-15
  - See also* WLST
- owc\_discussions, 1-6
- owc\_wiki, 1-6
- OWLCS
  - See* Oracle WebLogic Communications Server, 11-12

## P

- page management (WebCenter spaces), 20-1
- page permissions (WebCenter Spaces), 19-3
- Page service
  - performance issues and actions, 15-39
  - performance metrics, 15-27
- page styles (WebCenter Spaces), 18-19
- passwords, editing (WebCenter Spaces), 18-13

- PDK-Java producers, 12-8, A-15
- performance issues and actions, 15-39
  - Announcements service, 15-37
  - BPEL Worklists service, 15-37
  - Discussions service, 15-37
  - Documents service, 15-37
  - External Applications service, 15-38
  - Group Space Events service, 15-38
  - IMP service, 15-38
  - import and export, 15-38
  - Lists service, 15-38
  - Mail service, 15-38
  - Notes service, 15-39
  - Page service, 15-39
  - portlet producers, 15-39
  - RSS News Feed service, 15-39
  - Search service, 15-40
- performance metrics, 15-1
  - Announcements service, 15-9
  - common performance issues and actions, 15-7
  - Discussions service, 15-15
  - Documents service, 15-10
  - external applications, 15-19
  - Group Space Events service, 15-17
  - group spaces, 15-40
  - Import and Export service, 15-22
  - Instant Messaging and Presence service, 15-21
  - Lists service, 15-22
  - Mail service, 15-24
  - metrics common across WebCenter services, 15-3
  - most popular operations and response time, 15-3
  - Notes service, 15-26
  - Page service, 15-27
  - per operation metrics, 15-3
  - portlet producers, 15-28
  - portlets, 15-30
  - Recent Activities service, 15-34
  - recent history and since startup, 15-2
  - RSS News Feed service, 15-34
  - Search service, 15-35
  - services summary, 15-3
  - viewing performance, 15-42
  - Worklist service, 15-10
- permissions, 19-3
  - Discussions server, 19-5
  - Fusion Middleware Control, 1-10
  - WebCenter Spaces, 19-3
  - WebLogic Administration Server, 1-10
  - wiki and blog server, 11-67
- personal pages (WebCenter Spaces)
  - changing permissions, 20-13
  - copying, 20-15
  - default look and feel, 20-11
  - deleting, 20-16
  - editing, 20-12
  - managing, 20-10
  - restricting public access, 20-21
- personal spaces
  - enabling and disabling, 18-17
  - resource catalog customization, 18-20
- portalTools, 1-6
- portlet, A-17
- portlet producer applications
  - deploying, 7-1
  - undeploying, 7-29
- portlet producers, 15-39
  - about, 12-1
  - converting a JSR 168 portlet producer EAR file into a WSRP EAR file, 12-14
  - deleting producer connections using Fusion Middleware Control, 12-13
  - deleting producer connections using WLST, 12-13
  - deploying
    - deployment
      - portlet producers, 7-18
  - deploying portlet producer applications using Fusion Middleware Control, 12-15
  - deploying portlet producer applications using WebLogic Administration Console, 12-15
  - deploying portlet producer applications using WLST, 12-15
  - editing producer connection details using Fusion Middleware Control, 12-11
  - editing producer connection details using WLST, 12-12
  - managing post deployment
    - custom WebCenter applications, 6-6
    - WebCenter Spaces, 6-3
  - performance metrics, 15-28
  - registering Oracle PDK-Java producers using Fusion Middleware Control, 12-8
  - registering Oracle PDK-Java producers using WLST, 12-10
  - registering WSRP producers using Fusion Middleware Control, 12-2
  - registering WSRP producers using WLST, 12-7
  - troubleshooting, B-11
- portlets
  - adding to WebCenter Spaces resource catalog, 18-20
  - cache size, A-17
  - locale support, A-16
  - performance metrics, 15-30
  - timeouts, A-17
  - tuning, A-16
- POST Authentication Method, 13-6
- privacy statement (WebCenter Spaces), 18-7
- profile information (WebCenter Spaces)
  - allowing users to edit, 18-13
  - displaying, 18-13
  - managing permissions
    - Discussions service
      - permissions (WebCenter Spaces), 19-3
- public credentials, 13-7
- public Welcome page (WebCenter Spaces)
  - customizing default, 20-17
  - default, 20-18

Public-User role (WebCenter Spaces), 19-2  
granting permissions, 19-14

## R

---

RCU (Repository Creation Utility), 7-11  
Recent Activities service  
    performance metrics, 15-34  
Recent History metrics, 15-2  
redeployment  
    custom WebCenter applications, 7-1, 7-31  
    portlet producer applications, 7-1, 7-31  
    understanding, 7-32  
    using Fusion Middleware Control, 7-33  
    using WLST, 7-37  
removeExtAppCredential, 13-8  
removeExtAppField, 13-8  
Repository Creation Utility (RCU), 7-11  
resource catalog, customizing (WebCenter Spaces), 18-20  
roles and responsibilities, 3-2  
roles and responsibilities (WebCenter Spaces), 2-2, 3-1  
RSS News Feed service, A-14  
    configuring proxie, 11-73  
    performance issues and actions, 15-39  
    performance metrics, 15-34  
RTC Web service, 11-14

## S

---

Search service  
    connection  
        activating, 11-40  
        creating, 11-37  
        deleting, 11-42  
        managing, 11-36  
        modifying, 11-41  
    performance issues and actions, 15-40  
    performance metrics, 15-35  
Secure Enterprise Search  
    managing connections, 11-36  
    performance metrics, 15-35  
    prerequisites, 11-36  
    registering, 11-37  
    SSL security, 11-37  
security  
    ADF security, 14-3  
    administrator accounts, 14-4  
    default configuration, 14-4  
    external LDAP, 14-9  
    identity store, 14-5  
    Java Keystore, 14-186  
    keystores for WSRP producers, 14-185  
    managing, 14-1  
    Oracle Platform Security Services, 14-3  
    policy store, 14-5  
        configuring for OID, 14-37  
    single sign-on, 14-9  
    SSL, 14-9

WebCenter Security Framework, 14-3  
WebCenter Spaces, 14-3  
WebLogic Server security, 14-3  
WS-Security, 14-10  
Security Assertion Markup Language, 14-107  
    components, 14-107  
self-registration (WebCenter Spaces), 19-16  
    customizing Self-Registration page, 20-20  
    enabling by invitation, 19-16  
    enabling for anyone, 19-17  
Self-Registration page (WebCenter Spaces)  
    customizing default, 20-20  
    default, 20-20  
Services, 15-3  
services  
    *See* WebCenter services  
SES  
    *See* Secure Enterprise Search, 11-36  
session language (WebCenter Spaces), 18-8  
session timeout, A-8  
setBPELConnection (WLST command), 11-50  
setDiscussionForumConnection (WLST command), 11-8, 11-9  
setDocumentsSpacesProperties (WLST command), 10-20  
setDomainEnv.sh, A-7  
setExtAppConnection (WLST command), 13-8  
setExtAppCredential, 13-8  
setExtAppField, 13-8  
setIMailConnection (WLST command), 11-34  
setIMailConnectionProperty (WLST command), 11-34  
setIMPConnection (WLST command), 11-23, 11-24  
setIMPConnectionProperty (WLST command), 11-24  
setJCRContentServerConnection (WLST command), 10-17, 10-18  
setJCRFileSystemConnection (WLST command), 10-17, 10-18  
setJCRPortalConnection (WLST command), 10-17, 10-18  
setMailConnection (WLST command), 11-33  
setSearchConfig (WLST command), 11-42  
setSearchSESConfig (WLST command), 11-42  
setSESConnection (WLST command), 11-41, 11-42  
shared credentials, 13-7  
Sidebar (WebCenter Spaces)  
    Applications pane, 21-1  
    arranging applications, 21-6  
    customizing for everyone, 18-3  
    editing application links, 21-5  
    hiding and showing services, 18-4  
    hiding and showing task flows, 18-4  
    locking applications, 21-7  
    locking content, 18-4  
    making applications available, 21-2  
    removing application links, 21-8  
single sign-on  
    about, 14-9  
    BPEL server requirements, 11-45

- external applications, 13-4
- Microsoft clients, 14-155
- Oracle Access Manager, 14-72
- Oracle Application Server Single Sign-On, 14-100
- SAML-based, 14-107
- skins (WebCenter Spaces)
  - creating, 18-7
  - default, 18-6
  - selecting
    - application skins (WebCenter Spaces)
      - selecting**, 18-7
    - using, 18-6
- SMTP, 11-26
  - SSL security, 11-28
- SOA Suite, 9-1
- Spaces-User role (WebCenter Spaces), 19-1, 19-2
  - granting permissions, 19-14
- ssetRSSProxyConfig (WLST command), 11-73
- SSL security
  - about, 14-9
  - browser connection to custom WebCenter application, 14-50
  - browser connection to WebCenter Spaces, 14-42
  - browser connection to Wiki service, 14-54
  - IMAP connections, 11-28
  - Oracle Content Server, 10-5
  - Oracle HTTP Server to WebCenter Spaces, 14-50
  - OWLCS connections, 11-14
  - SES connections, 11-37
  - SMTP connections, 11-28
  - WebCenter Spaces connection to
    - IMAP/SMTP, 14-69
    - WebCenter Spaces connection to LCS, 14-71
    - WebCenter Spaces connection to LDAP, 14-68
    - WebCenter Spaces connection to OCS, 14-69
    - WebCenter Spaces connection to OWLCS, 14-70
    - WebCenter Spaces connection to portlet producers, 14-60
    - WebCenter Spaces connection to SES, 14-70
- startApplication (WLST command), 8-4, 8-5
- startNodeManager.sh, 8-2
- StartScriptEnabled, 8-2
- stopApplication (WLST command), 8-5, 8-6
- subscription workflows, 9-1
- system libraries, 1-5, 1-6
- system limit, A-6
- Systems MBean Browser, A-5

## T

---

- Tags service
  - managing connection, 11-51, 11-53
- task flows
  - adding to WebCenter Spaces resource catalog, 18-20
  - availability in WebCenter Spaces, 18-15
  - hiding and showing in Sidebar, 18-4
  - hiding for disabled services, 18-16
  - launching from WebCenter Spaces Sidebar, 21-2
- template (wiki), creating a template, 11-64

- templates (WebCenter Spaces)
  - deleting, 22-8
  - exporting, 23-6
  - importing, 23-7
  - managing, 22-7
  - publishing and unpublishing, 22-9
  - viewing, 22-7
- templates (WebCenter Spaces), customizing, 18-18
- themes (wiki), changing a theme, 11-64
- timeouts
  - concurrency management, A-10
  - HTTP session, A-8
  - JSP page, A-9
  - portlets, A-17
  - services and portlets, A-11
- troubleshooting
  - Discussions service, B-7
  - IMP service, B-8
  - Mail service, B-9
  - Oracle WebCenter Wiki and Blog Server, B-12
  - portlet producers, B-11
  - WebCenter application configuration, B-1
  - WebCenter applications, B-1
  - WebCenter Spaces export, B-20
  - WLST, B-4
  - Worklist service, B-13
- tuning, A-12, A-13, A-14, A-15

## U

---

- undeployment
  - custom WebCenter applications, 7-1, 7-29
  - portlet producer applications, 7-1, 7-29
  - using Fusion Middleware Control, 7-29
  - using WLST, 7-30
- UPLOAD\_MAX\_DISK\_SPACE, A-4
- UPLOAD\_MAX\_MEMORY, A-4
- UPLOAD\_TEMP\_DIR, A-4
- user-defined roles (WebCenter Spaces), 19-3
- users (WebCenter Spaces)
  - adding and removing, 19-11
  - assigning to roles, 19-7
  - changing roles, 19-8
  - granting administrator role, 19-10
  - managing, 14-41, 19-6
  - revoking roles, 19-10
  - Spaces-User role, 19-6

## W

---

- wc\_domain, 1-4
- wc.chromeLevel, 18-18
- webcenter (J2EE application), 1-6
- WebCenter Applications
  - single sign-on, 14-72
- WebCenter applications
  - administrator accounts, 14-4
  - configuration changes, A-5
  - configuration tools, A-5
  - default security, 14-4

- identity store, 14-5
- managing security, 14-1
- policy store, 14-5
- See also* custom WebCenter applications
- tuning, A-6, A-8
- WebCenter Composer, 1-3
- WebCenter Framework, 1-2
- WebCenter repository
  - configuring, 11-51
- WebCenter services
  - enabling and disabling in WebCenter Spaces, 18-15, 22-6
  - hiding and showing in Sidebar, 18-4
  - hiding task flows for disabled services, 18-16
  - reporting issues, 18-16
  - setting up connections, 11-1
- WebCenter Spaces
  - about, 1-3
  - administering applications (checklist), 3-1
  - Administration pages, 1-11, 17-1
  - application roles, 14-4
  - Applications pane, 21-1
  - Application-View permission, 18-17
  - changing application name, 18-1
  - configuring WS-Security, 14-168
  - customizing, 18-1
    - application templates, 18-18
    - copyright and privacy statements, 18-7
    - Login page, 20-18
    - page styles, 18-19
    - public Welcome page, 20-17
    - Self-Registration page, 20-20
    - skins, 18-6
  - default display language, 18-8
  - enabling services, 18-15
  - enterprise roles, 14-4
  - exporting and importing, 16-1
  - exporting group space templates, 16-32
  - exporting group spaces, 16-31
  - getting the application up and running (checklist), 2-1
  - home page in Fusion Middleware Control, 6-2
  - importing group space templates, 16-33
  - importing group spaces, 16-32
  - logging in as Administrator, 17-1
  - logo, 18-5
  - logs, 15-44
  - making applications available, 21-2
  - managing users and roles, 19-1
  - monitoring performance, 15-1, 15-42
  - permissions, 19-3
  - policy store permissions, 14-6
  - security, 14-2, 14-3
    - granting admin role, 14-31
  - starting and restarting
    - using Fusion Middleware Control, 8-4
    - using WLST, 8-4
  - stopping
    - using Fusion Middleware Control, 8-4
    - using WLST, 8-5
  - viewing and configuring logs, 15-44
  - WebDAV URL, 18-17
- WebCenter Spaces administrators, 2-2, 3-2
- WebCenter Web 2.0 Services, 1-3
- webcenter-help, 1-6
- WebDAV URL, 18-17
- WebLogic Administration Console
  - about, 1-13
  - deploying portlet producer applications, 12-15
  - operation summary, 1-11
- WebLogic Managed Server
  - creating, 7-2
  - provisioning, 7-2
- WebLogic Server security, 14-3
- web.xml, A-1, A-4
- Welcome page (WebCenter Spaces)
  - customizing default, 20-17
  - default, 20-18
- wiki pages
  - deleting, 11-69
  - naming convention, 11-62
  - unlocking, 11-65
- Wiki service, configuration, 11-53
- WLS Administration Console
  - deploying custom WebCenter applications, 7-26
  - deploying portlet producer applications, 7-26
  - managed server, creating, 7-3
- WLS\_Custom-diagnostics.log, 15-44
- WLS\_Portlets, 1-5
- WLS\_Services, 1-5
- WLS\_Spaces, 1-5
- WLS\_Spaces-diagnostic.log, 15-44
- WLST
  - addWorklistConnection, 11-49
  - changing content repository active connection, 10-17
  - createBPELConnection, 11-48
  - createIMPConnection, 11-22
  - createJCRContentServerConnection, 10-15
  - createJCRFileSystemConnection, 10-15
  - createJCRPortalConnection, 10-15
  - createMailConnection, 11-32
  - createSESSConnection, 11-40
  - deleteConnection, 10-19, 11-11, 11-26, 11-35, 11-43, 11-51, 13-9
  - deleteDocumentsSpacesProperties, 10-20
  - deleting content repository connections, 10-19
  - deleting producer connections, 12-13
  - deploying custom WebCenter applications, 7-24
  - deploying portlet producer applications, 12-15
  - editing producer connection details, 12-12
  - exporting group space templates, 16-32
  - exporting group spaces, 16-31
  - exporting portlet client metadata, 16-35
  - exporting WebCenter Spaces, 16-20
  - exporting WebCenter Web 2.0 Services metadata and data, 16-36
  - getRSSProxyConfig, 11-73
  - importing group space templates, 16-33
  - importing group spaces, 16-32

- importing portlet client metadata, 16-35
- importing WebCenter Spaces, 16-22
- importing WebCenter Web 2.0 Services metadata and data, 16-38
- listDocumentsSpacesProperties, 10-20
- managing content repository connection properties (WebCenter Spaces), 10-20
- migrating custom WebCenter application security policies, 16-39
- modifying content repository connection details, 10-18
- operation summary, 1-11
- redeploying custom WebCenter applications, 7-37
- redeploying portlet producer applications, 7-37
- registering an MDS schema, 7-17
- registering content repositories, 10-15
- registering Oracle PDK-Java producers, 12-10
- registering WSRP producers, 12-7
- removeExtAppCredential, 13-8
- removeExtAppField, 13-8
- removeWorklistConnection, 11-49
- setBPELConnection, 11-50
- setDiscussionForumConnection, 11-8, 11-9
- setDocumentsSpacesProperties, 10-20
- setExtAppConnection, 13-8
- setExtAppCredential, 13-8
- setExtAppField, 13-8
- setIMPConnection, 11-23, 11-24
- setIMPConnectionProperty, 11-24
- setJCRContentServerConnection, 10-17, 10-18
- setJCRFileSystemConnection, 10-17, 10-18
- setJCRPortalConnection, 10-17, 10-18
- setMailConnection, 11-33, 11-34
- setMailConnectionProperty, 11-34
- setRSSProxyConfig, 11-73
- setSearchConfig, 11-42
- setSearchSESSConfig, 11-42
- setSESSConnection, 11-41, 11-42
- startApplication, 8-4
- stopApplication, 8-5
- undeploying custom WebCenter applications, 7-30
- undeploying portlet producer applications, 7-30
- wlst.sh, 1-15
- workflows
  - WebCenter Spaces workflows, 9-1
- Worklist service
  - connection
    - activating, 11-48
    - creating, 11-45
    - deleting, 11-50
    - managing, 11-43
    - modifying, 11-49
  - performance metrics, 15-10
  - troubleshooting, B-13
  - WebCenter Spaces workflows, 9-1
- wsm-pm, 1-6
- WSRP producers, A-15
  - keystores, 14-185
  - registering, 12-2
  - WS-Security, 14-180
- wsrp-tools, 1-6
- WS-Security
  - about, 14-10
  - BPEL server, 11-45, 14-168
  - configuring, 14-168
  - Discussions server, 11-3, 14-176
  - Discussions server connections, 14-176
  - OWLCS, 11-14, 14-178
  - WSRP producers, 14-180