

Oracle® Fusion Middleware

Administrator's Guide for Oracle WebCenter Portal

11g Release 1 (11.1.1.6.0)

E12405-18

December 2012

Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal, 11g Release 1 (11.1.1.6.0)

E12405-18

Copyright © 2007, 2012, Oracle and/or its affiliates. All rights reserved.

Primary Author: Rosie Harvey

Contributing Authors: Ingrid Snedecor, Joan Carter, Michele Cyran, Peter Jacobsen, Promila Chitkara, Sarah Bernau, Savita Thakur, Sue Highmoor

Contributor: Alan Jalife, Alison Macmillan, Alistair Wilson, Annesharmila Immanueljoseph, Artem Stemkovski, Avinash Rajendran, Chandrasaha Peddamallu, Chris Bales, Christian Hauser, Chung Cheng, Corinne Pelote, Dan Mullen, David Pattelena, Diego Sabaris, Harsha Ramesh, Howard Wu, Gaston Martino, Greg Gutkin, Igor Polyakov, Jamie Lord, Jeff Prehm, Jeni Ferns, John Whiting, Karl Bilawski, Ken Young, Kim-Phung Dinh, Lei Oh, Madhu Muppagowni, Mahima Subbaraman, Manish Devgan, Marcus Diaz, Mark Rossi, Michele Chen Chock, Nagaraju Suravarjjala, Nazar Doroshenko, Nicolas Pombourcq, Nitin Shah, Pankaj Mittal, Preeti Yarashi, Pushkar Kapasi, Rahmath Baig, Ravi Baranwal, Rich Nessel, Robin Fisher, Rohit Kularni, Roopam Bahl, Sachin Parashar, Sarah Maslin, Seshan Kannan, Shin Huang, Shakeb Sagheer, Shaolin Shen, Sharmila Jayaram, Sunil Franklin, Stephen Thornhill, Steve Roth, Tim Lake, Yueh-Hong Lin, Vaibhav Lole, Ved Singh, Vineet Duggal

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

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

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

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

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

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

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

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

Contents

Preface	xxxiii
Audience	xxxiii
Documentation Accessibility	xxxiii
Related Documents	xxxiii
Conventions	xxxiv
What's New	xxxv
New Features for Release 11.1.1.6	xxxv
 Part I Understanding Oracle WebCenter Portal	
 1 Introduction to Oracle WebCenter Portal Administration	
1.1 Introducing Oracle WebCenter Portal	1-1
1.2 Oracle WebCenter Portal Architecture	1-2
1.2.1 WebCenter Portal: Framework	1-3
1.2.2 Application Development Framework	1-3
1.2.3 Composer	1-3
1.2.4 WebCenter Portal: Spaces	1-4
1.2.5 WebCenter Portal: Services	1-4
1.2.6 Discussion Server	1-5
1.2.7 Analytics	1-5
1.2.8 Activity Graph	1-5
1.2.9 Personalization Server	1-5
1.2.10 Portals	1-5
1.2.11 Composite Applications	1-5
1.3 Oracle WebCenter Portal Topology	1-6
1.3.1 WebCenter Portal Topology Out-of-the-Box	1-6
1.3.2 WebCenter Portal Managed Servers	1-7
1.3.3 WebCenter Portal Startup Order	1-8
1.3.4 WebCenter Portal Dependencies	1-8
1.3.5 WebCenter Portal Configuration Considerations	1-9
1.3.6 WebCenter Portal State and Configuration Persistence	1-10
1.3.7 WebCenter Portal Log File Locations	1-11
1.4 Spaces Application	1-12
1.5 Framework Applications	1-12

1.6	Planning WebCenter Portal Installations	1-13
1.7	Understanding the WebCenter Portal 11g Installation	1-13
1.8	Understanding Administrative Operations, Roles, and Tools	1-13
1.9	Performance Monitoring and Diagnostics	1-15
1.10	Understanding Security	1-15
1.11	WebCenter Portal Application Deployment	1-15
1.12	Data Migration, Backup, and Recovery	1-16
1.13	Oracle WebCenter Portal Administration Tools	1-16
1.13.1	Oracle Enterprise Manager Fusion Middleware Control Console	1-16
1.13.1.1	Displaying Fusion Middleware Control Console	1-17
1.13.2	Oracle WebLogic Server Administration Console	1-17
1.13.3	Oracle WebLogic Scripting Tool (WLST)	1-18
1.13.3.1	Running Oracle WebLogic Scripting Tool (WLST) Commands	1-18
1.13.4	System MBean Browser	1-20
1.13.5	Spaces Administration Pages	1-21
1.13.6	WebCenter Portal Administration Console	1-22

Part II Getting Started With Oracle WebCenter Portal Administration

2 Getting the Spaces Application Up and Running

2.1	Role of the Fusion Middleware Administrator	2-1
2.2	Role of the Spaces Administrator	2-2
2.3	Installing WebCenter Portal: Spaces	2-2
2.4	Setting Up Spaces for the First Time (Roadmap)	2-3
2.5	Customizing Spaces for the First Time (Roadmap)	2-5

3 Maintaining the Spaces Application

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

4 Getting Framework Applications Up and Running

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

5 Maintaining Framework Applications

5.1	System Administration for Framework Applications (Roadmap)	5-1
-----	--	-----

Part III Basic Systems Administration for Oracle WebCenter Portal

6 Starting Enterprise Manager Fusion Middleware Control

6.1	Displaying Fusion Middleware Control Console	6-1
6.2	Navigating to the Home Page for the Spaces Application	6-2
6.3	Navigating to the Home Page for Framework Applications	6-5

6.4	Navigating to Dependent Components	6-7
-----	--	-----

7 Deploying WebCenter Portal: Framework Applications

7.1	Deploying Framework applications	7-1
7.1.1	Deployment Roadmap	7-2
7.1.2	Deployment Prerequisites	7-3
7.1.3	Preparing the Application EAR File	7-4
7.1.3.1	EAR File Contents	7-4
7.1.4	Creating a Managed Server	7-4
7.1.5	Creating and Registering the Metadata Service Repository	7-5
7.1.5.1	Creating an MDS Schema Using the Repository Creation Utility	7-5
7.1.5.2	Registering an MDS Schema Using Fusion Middleware Control	7-9
7.1.5.3	Registering an MDS Schema Using WLST	7-11
7.1.6	Deploying the Application to a WebLogic Managed Server	7-12
7.1.6.1	Choosing the Information Artifact Store	7-12
7.1.6.2	Choosing the Data Source	7-13
7.1.6.3	Deploying Applications Using Oracle JDeveloper	7-14
7.1.6.4	Deploying Applications Using Fusion Middleware Control	7-14
7.1.6.5	Deploying Applications Using WLST	7-19
7.1.6.6	Deploying Applications Using the WLS Administration Console	7-21
7.1.6.7	Saving and Reusing the Deployment Plan	7-24
7.1.7	Migrating Customizations and Data Between Environments	7-24
7.1.8	Configuring Applications to Run in a Distributed Environment	7-25
7.2	Undeploying Framework applications	7-25
7.2.1	Undeploying Framework Applications Using Fusion Middleware Control	7-25
7.2.2	Undeploying Framework Applications Using WLST	7-25
7.2.3	Removing an Application's Credential Map	7-26
7.3	Redeploying Framework applications	7-27
7.3.1	Redeployment Considerations	7-28
7.3.1.1	Preserving Application Configuration	7-28
7.3.1.1.1	Preserving Configuration Across Deployment Using WLST	7-29
7.3.1.2	Preserving Service and User Customizations	7-29
7.3.1.3	Preserving Resource Customizations	7-29
7.3.1.4	Preserving Portlet Customizations	7-30
7.3.2	Redeploying Framework Applications Using Fusion Middleware Control	7-30
7.3.3	Redeploying Framework Applications Using WLST	7-34
7.4	Post-Deployment Configuration	7-35
7.4.1	Checking Security Configurations After Deployment	7-35
7.4.2	Checking Application Connections After Deployment	7-36
7.4.3	Checking Data Source Connections	7-36
7.4.4	Tuning the Application	7-36

8 Starting and Stopping WebCenter Portal Applications

8.1	Starting Node Manager	8-2
8.2	Starting and Stopping Managed Servers for WebCenter Portal Application Deployments ..	8-2

8.3	Starting and Stopping the Spaces Application	8-4
8.3.1	Starting Spaces Using Fusion Middleware Control	8-4
8.3.2	Starting Spaces Using WLST	8-4
8.3.3	Stopping Spaces Using Fusion Middleware Control	8-5
8.3.4	Stopping Spaces Using WLST	8-5
8.4	Starting and Stopping Framework Applications	8-5
8.4.1	Starting Framework Applications Using Fusion Middleware Control	8-6
8.4.2	Starting Framework Applications Using WLST	8-6
8.4.3	Stopping Framework Applications Using Fusion Middleware Control	8-6
8.4.4	Stopping Framework Applications Using WLST	8-7

9 Setting WebCenter Portal Application Properties

9.1	Setting Application Properties for the Spaces Application	9-1
9.2	Setting Application Properties for Framework Applications	9-2
9.3	Specifying the BPEL Server Hosting Spaces Workflows	9-2
9.4	Configuring Search Crawlers	9-3
9.5	Setting Search Options	9-4
9.6	Choosing a Channel for Notification Messages	9-4
9.7	Setting Up a Proxy Server	9-5
9.7.1	Setting Up a Proxy Server Using Fusion Middleware Control	9-5
9.7.2	Setting Up a Proxy Server Using WLST	9-5
9.8	Exposing Spaces Templates From a Previous Release	9-6
9.9	Setting a Session Timeout for the Spaces Application	9-7

Part IV Managing Services, Portlet Producers, and External Applications

10 Managing Oracle WebCenter Portal Services

10.1	Introduction to Managing Services	10-1
10.1.1	Setting Up the MDS Repository	10-4
10.1.2	Setting Up Database Connections	10-4
10.1.3	Setting Up External Application Connections	10-5

11 Managing Content Repositories

11.1	What You Should Know About Content Repositories	11-1
11.2	Configuring Oracle WebCenter Content Server Repositories	11-3
11.2.1	Prerequisites to Configuring Content Server	11-3
11.2.1.1	Installation Prerequisites	11-4
11.2.1.2	Configuration Prerequisites	11-4
11.2.1.3	Security Prerequisites	11-5
11.2.2	Configuration Roadmap for Content Server	11-5
11.2.3	Configuring Content Server for WebCenter Portal Applications	11-9
11.2.3.1	Enabling Mandatory Components	11-9
11.2.3.1.1	What You Should Know About the WebCenterConfigure Component ...	11-10
11.2.3.2	Configuring the Dynamic Converter Component	11-12
11.2.3.3	Configuring the Inbound Refinery	11-13
11.2.3.3.1	Creating an Outbound Provider	11-13

11.2.3.3.2	Enabling PDFExportConverter in Inbound Refinery	11-14
11.2.3.3.3	Selecting the File Formats To Be Converted	11-15
11.2.3.3.4	Enabling the Conversion of Wikis and Blogs into PDFs	11-16
11.2.3.4	Setting Up SSL for Content Server	11-17
11.2.3.5	Enabling the iFraming UI in WebCenter Portal	11-17
11.2.3.6	Configuring the SES Crawler	11-18
11.2.3.7	Setting Up Site Studio	11-18
11.2.3.8	Enabling OracleTextSearch	11-19
11.2.3.9	Creating Content Profiles in Content Server	11-19
11.2.3.10	Configuring Item Level Security in WebCenter Portal Applications	11-20
11.2.3.10.1	What You Should Know About Item Level Security	11-20
11.2.3.10.2	Configuring Item Level Security	11-22
11.2.3.10.3	Configuring Additional Settings for WebCenter Portal: Framework Applications	11-23
11.2.3.11	Additional Optional Configurations	11-23
11.2.3.11.1	Configuring the File Store Provider	11-23
11.2.3.11.2	Setting Up Node Manager	11-24
11.2.3.12	Configuring Security Between Content Server and WebCenter Portal: Framework Applications	11-24
11.2.3.12.1	Creating a Security Group Using the Content Server Console	11-25
11.2.3.12.2	Creating Roles Using the Content Server Console	11-26
11.2.3.12.3	Creating Roles (Groups) Using Fusion Middleware Control	11-26
11.2.3.12.4	Creating a Folder Using the Content Server Console	11-27
11.2.3.12.5	Creating Users Using Fusion Middleware Control	11-27
11.2.3.12.6	Granting a Role to a User Using Fusion Middleware Control	11-28
11.2.3.12.7	Migrating Security to a Production Environment	11-28
11.2.3.12.8	Checking Your Security Group and Roles Configuration	11-28
11.2.3.13	Registering the Content Server Connection	11-29
11.2.3.13.1	Configuring the Content Server Connection for Framework Applications	11-29
11.2.3.13.2	Configuring the Content Server Connection for Spaces	11-29
11.2.3.13.3	Checking the Spaces Data Seeded in Content Server	11-30
11.3	Configuring Microsoft SharePoint Repositories	11-32
11.3.1	Microsoft SharePoint - Installation	11-33
11.3.1.1	What You Should Know About Microsoft SharePoint Server Installation	11-33
11.3.1.2	Installing Oracle WebCenter Adapter for Microsoft SharePoint	11-33
11.3.1.3	Installing WLST Command Scripts for Managing Microsoft SharePoint Connections	11-35
11.3.2	Microsoft SharePoint - Configuration	11-35
11.3.3	Microsoft SharePoint - Security Considerations	11-35
11.3.4	Microsoft SharePoint - Limitations in WebCenter Portal	11-36
11.3.5	Managing Microsoft SharePoint Connections Using WLST	11-36
11.3.5.1	createJCRSharePointConnection	11-36
11.3.5.2	setJCRSharePointConnection	11-36
11.3.5.3	listJCRSharePointConnections	11-37
11.4	Configuring Oracle Portal Repositories	11-37
11.4.1	Oracle Portal - Installation	11-37
11.4.2	Oracle Portal - Configuration	11-37

11.4.3	Oracle Portal - Security Considerations	11-37
11.4.4	Oracle Portal - Limitations in WebCenter Portal	11-37
11.5	Configuring a File System Repository	11-38
11.5.1	File System - Security Considerations	11-38
11.5.2	File System - Limitations in WebCenter Portal	11-38
11.6	Registering Content Repositories	11-38
11.6.1	What You Should Know About Registering Content Repositories for Spaces	11-39
11.6.2	Registering Content Repositories Using Fusion Middleware Control	11-40
11.6.3	Registering Content Repositories Using WLST	11-48
11.7	Changing the Active (or Default) Content Repository Connection	11-48
11.7.1	Changing the Active (or Default) Content Repository Connection Using Fusion Middleware Control	11-49
11.7.2	Changing the Active (or Default) Content Repository Connection Using WLST ..	11-49
11.8	Modifying Content Repository Connection Details	11-50
11.8.1	Modifying Content Repository Connection Details Using Fusion Middleware Control 11-50	
11.8.2	Modifying Content Repository Connection Details Using WLST	11-50
11.8.3	Modifying Cache Settings for Content Presenter	11-51
11.9	Deleting Content Repository Connections	11-55
11.9.1	Deleting Content Repository Connections Using Fusion Middleware Control	11-55
11.9.2	Deleting Content Repository Connections Using WLST	11-55
11.10	Setting Connection Properties for the Spaces Content Repository	11-56
11.10.1	Setting Connection Properties for the Spaces Content Repository Using Fusion Middleware Control	11-56
11.10.2	Setting Connection Properties for the Spaces Content Repository Using WLST ...	11-56
11.11	Testing Content Repository Connections	11-57
11.11.1	Testing Content Server Connections	11-57
11.11.2	Testing Oracle Portal Connections	11-58
11.12	Changing the Maximum File Upload Size	11-59

12 Managing the Activity Graph Service

12.1	What You Should Know About the Activity Graph Service	12-1
12.2	Configuration Roadmaps for the Activity Graph Service	12-4
12.3	Activity Graph Service Prerequisites	12-7
12.4	Preparing Data for the Activity Graph Service	12-8
12.4.1	Running the Activity Graph Engines on a Schedule	12-9
12.4.2	Running the Activity Graph Engines on Demand	12-9
12.5	Customizing Reason Strings for Similarity Calculations	12-10
12.6	Managing Activity Graph Schema Customizations	12-11
12.6.1	Exporting Activity Graph Metadata	12-11
12.6.2	Exporting Provider Configuration	12-12
12.6.3	Importing Activity Graph Metadata	12-12
12.6.4	Deleting Activity Graph Metadata	12-12
12.6.5	Renaming Actions and Node Classes	12-13
12.7	Setting Up Activity Rank for Oracle Secure Enterprise Search	12-13
12.8	Troubleshooting Issues with Recommendations	12-16
12.8.1	Troubleshooting the Activity Graph Engines Schedule and Status Page	12-17

13 Managing the Analytics Service

13.1	What You Should Know About Analytics in WebCenter Portal	13-2
13.1.1	Analytics Components	13-2
13.1.2	Analytics Task Flows	13-3
13.2	Configuration Roadmap for the Analytics Service	13-4
13.3	Analytics Prerequisites	13-5
13.3.1	Analytics - Installation	13-5
13.3.2	Analytics - Configuration	13-5
13.3.3	Analytics - Security Considerations	13-5
13.3.4	Analytics - Limitations	13-6
13.4	Configuring Analytics Collector Settings	13-6
13.4.1	Setting Analytics Collector Properties Using WLST	13-6
13.4.2	Setting Analytics Collector Properties Using Fusion Middleware Control	13-7
13.5	Registering an Analytics Collector for Your Application	13-9
13.5.1	Registering an Analytics Collector Using Fusion Middleware Control	13-9
13.5.2	Registering an Analytics Collector Using WLST	13-10
13.5.3	Disabling WebCenter Event Collection	13-11
13.5.3.1	Disabling WebCenter Portal Event Collection Using Fusion Middleware Control .. 13-11	
13.5.3.2	Disabling WebCenter Portal Event Collection Using WLST	13-12
13.6	Configuring User Profile Events Timing	13-12
13.7	Validating Analytic Event Collection	13-12
13.8	Viewing the Current WebCenter Portal's Analytic Event List	13-13
13.9	Purging Analytics Data	13-14
13.10	Partitioning Analytics Data	13-14
13.11	Troubleshooting Issues with Analytics	13-14

14 Managing the Announcements and Discussions Services

14.1	What You Should Know About Discussions Server Connections	14-2
14.2	Discussions Server Prerequisites	14-2
14.2.1	Discussions Server - Installation	14-2
14.2.1.1	Discussions Server - High Availability Installation	14-3
14.2.2	Discussions Server - Configuration	14-3
14.2.3	Discussions Server - Security Considerations	14-4
14.2.4	Discussions Server - Limitations	14-5
14.3	Registering Discussions Servers	14-5
14.3.1	Registering Discussions Servers Using Fusion Middleware Control	14-5
14.3.2	Registering Discussions Servers Using WLST	14-9
14.4	Choosing the Active Connection for Discussions and Announcements	14-10
14.4.1	Choosing the Active Connection for Discussions and Announcements Using Fusion Middleware Control	14-10
14.4.2	Choosing the Active Discussion for Discussions and Announcements Using WLST	14-10
14.5	Modifying Discussions Server Connection Details	14-11
14.5.1	Modifying Discussions Server Connection Details Using Fusion Middleware Control .. 14-11	
14.5.2	Modifying Discussions Server Connection Details Using WLST	14-12

14.6	Deleting Discussions Server Connections	14-12
14.6.1	Deleting a Discussions Server Connection Using Fusion Middleware Control	14-12
14.6.2	Deleting a Discussions Server Connection Using WLST	14-13
14.7	Setting Up Discussions Service Defaults	14-13
14.8	Setting Up Announcements Service Defaults	14-14
14.9	Testing Discussions Server Connections	14-14
14.10	Granting Administrator Permissions on the Discussions Server	14-14
14.11	Granting Administrator Role on the Discussions Server	14-15
14.11.1	Granting the Discussions Server Administrator Role using WLST	14-15
14.11.2	Granting the Discussions Server Administrator Role using the Admin Console ..	14-15
14.11.3	Revoking the Discussions Server Administrator Role	14-16
14.12	Troubleshooting Issues with Announcements and Discussions	14-17
14.12.1	Authentication Failed	14-17
14.12.2	Discussions Cannot Be Enabled in a Space	14-17
14.12.3	Login Failed	14-18
14.12.4	Login Does Not Function Properly After Configuring Oracle Access Manager	14-19
14.12.5	Category Not Found Exceptions	14-19

15 Managing the Events Service

15.1	What You Should Know About Events Connections	15-2
15.2	Configuration Roadmaps for Personal Events in the Events Service	15-2
15.3	Events Service Prerequisites for Personal Events	15-5
15.3.1	Microsoft Exchange Server 2007 Prerequisites	15-5
15.3.1.1	Microsoft Exchange Server 2007 - Installation	15-5
15.3.1.2	Microsoft Exchange Server 2007 - Configuration	15-6
15.3.1.3	Microsoft Exchange Server 2007 - Security Considerations	15-6
15.3.1.4	Microsoft Exchange Server 2007 - Limitations	15-7
15.3.2	Microsoft Exchange Server 2003 Prerequisites	15-7
15.3.2.1	Microsoft Exchange Server 2003 - Installation	15-7
15.3.2.2	Microsoft Exchange Server 2003 - Configuration	15-7
15.3.2.3	Microsoft Exchange Server 2003 - Security Considerations	15-8
15.3.2.4	Microsoft Exchange Server 2003 - Limitations	15-8
15.4	Registering Events Servers	15-8
15.4.1	Registering Events Servers Using Fusion Middleware Control	15-8
15.4.2	Registering Event Servers Using WLST	15-10
15.5	Choosing the Active Events Server Connection	15-10
15.5.1	Choosing the Active Events Server Using Fusion Middleware Control	15-10
15.5.2	Choosing the Active Events Server Connection Using WLST	15-11
15.6	Modifying Events Server Connection Details	15-11
15.6.1	Modifying Events Server Connection Details Using Fusion Middleware Control	15-12
15.6.2	Modifying Events Server Connection Details Using WLST	15-12
15.7	Deleting Event Server Connections	15-12
15.7.1	Deleting Event Server Connections Using Fusion Middleware Control	15-13
15.7.2	Deleting Event Server Connections Using WLST	15-13
15.8	Testing Event Server Connections	15-13
15.9	Troubleshooting Issues with Events	15-14

16 Managing the Instant Messaging and Presence Service

16.1	What You Should Know About Instant Messaging and Presence Connections	16-2
16.2	Instant Messaging and Presence Server Prerequisites	16-2
16.2.1	Microsoft Live Communications Server (LCS) Prerequisites	16-2
16.2.1.1	Microsoft LCS - Installation	16-2
16.2.1.2	Microsoft LCS - Configuration	16-2
16.2.1.3	Microsoft LCS - Security Considerations	16-5
16.2.2	Microsoft Office Communications Server (OCS) Prerequisites	16-6
16.2.2.1	Microsoft OCS - Installation	16-6
16.2.2.2	Microsoft OCS - Configuration	16-6
16.2.2.2.1	Simple Deployment	16-6
16.2.2.2.2	Remote Deployment	16-6
16.2.2.2.3	Building Application Provisioner	16-7
16.2.2.2.4	Provisioning WebCenter Portal's Proxy Application on OCS Server	16-8
16.2.2.2.5	IIS Server Configuration	16-8
16.2.2.2.6	Installing UCMA v2.0	16-9
16.2.2.2.7	Installing WebCenter Portal's Proxy Application	16-10
16.2.2.3	Microsoft OCS - Security Considerations	16-11
16.2.3	Microsoft Lync Prerequisites	16-11
16.2.3.1	Microsoft Lync - Installation	16-11
16.2.3.2	Microsoft Lync - Configuration	16-11
16.2.3.2.1	Simple Deployment	16-11
16.2.3.2.2	Remote Deployment	16-12
16.2.3.2.3	Building Application Provisioner	16-13
16.2.3.2.4	Provisioning WebCenter Portal's Proxy Application on Lync Server	16-14
16.2.3.2.5	Adding AllowedDomains Using WBemTest	16-14
16.2.3.2.6	Migrating Trusted Service Entries Using Topology Builder or PowerShell Cmdlets	16-15
16.2.3.2.7	IIS Server Configuration	16-16
16.2.3.2.8	Installing UCMA v2.0	16-17
16.2.3.2.9	Installing WebCenter Portal's Proxy Application	16-17
16.2.3.3	Microsoft Lync - Security Considerations	16-18
16.3	Registering Instant Messaging and Presence Servers	16-18
16.3.1	Registering Instant Messaging and Presence Servers Using Fusion Middleware Control	16-18
16.3.2	Registering Instant Messaging and Presence Servers Using WLST	16-21
16.4	Choosing the Active Connection for Instant Messaging and Presence	16-21
16.4.1	Choosing the Active Connection for Instant Messaging and Presence Using Fusion Middleware Control	16-21
16.4.2	Choosing the Active Connection for Instant Messaging and Presence Using WLST	16-22
16.5	Modifying Instant Messaging and Presence Connection Details	16-22
16.5.1	Modifying Instant Messaging and Presence Connections Details Using Fusion Middleware Control	16-23
16.5.2	Modifying Instant Messaging and Presence Connections Details Using WLST	16-23
16.6	Deleting Instant Messaging and Presence Connections	16-23

16.6.1	Deleting Instant Messaging and Presence Connections Using Fusion Middleware Control	16-24
16.6.2	Deleting Instant Messaging and Presence Connections Using WLST	16-24
16.7	Setting Up Instant Messaging and Presence Service Defaults	16-24
16.8	Testing Instant Messaging and Presence Connections	16-25

17 Managing the Mail Service

17.1	What You Should Know About Mail Server Connections	17-2
17.2	Configuration Roadmaps for the Mail Service	17-2
17.3	Mail Server Prerequisites	17-5
17.3.1	Mail Server - Installation	17-6
17.3.2	Mail Server - Configuration	17-6
17.3.2.1	Configuring Microsoft Exchange Server 2007 or 2010 for WebCenter Portal	17-6
17.3.2.1.1	Obtain the Certificate from the Microsoft Exchange Server	17-6
17.3.2.1.2	Add the Certificate to the WebCenter Portal Keystore	17-7
17.3.2.1.3	Microsoft Exchange Server Considerations	17-7
17.3.3	Mail Server - Security Considerations	17-8
17.3.4	Mail Server - Limitations	17-8
17.4	Registering Mail Servers	17-8
17.4.1	Registering Mail Servers Using Fusion Middleware Control	17-8
17.4.2	Registering Mail Servers Using WLST	17-12
17.5	Choosing the Active (or Default) Mail Server Connection	17-13
17.5.1	Choosing the Active (or Default) Mail Server Connection Using Fusion Middleware Control	17-14
17.5.2	Choosing the Active (or Default) Mail Server Connection Using WLST	17-14
17.6	Modifying Mail Server Connection Details	17-15
17.6.1	Modifying Mail Server Connection Details Using Fusion Middleware Control	17-15
17.6.2	Modifying Mail Server Connection Details Using WLST	17-15
17.7	Deleting Mail Server Connections	17-16
17.7.1	Deleting a Mail Connection Using Fusion Middleware Control	17-16
17.7.2	Deleting a Mail Connection Using WLST	17-17
17.8	Setting Up Mail Service Defaults	17-17
17.9	Testing Mail Server Connections	17-17
17.10	Troubleshooting Issues with Mail	17-18
17.10.1	Mail Service is Not Accessible in Secure Mode	17-18
17.10.2	Mail Service is Not Accessible in Non-Secure Mode	17-18
17.10.3	Unable to Create Distribution Lists in the Non-Secure Mode	17-19
17.10.4	Unable to Create Distribution Lists in the Secure Mode	17-19
17.10.5	Unable to Configure the Number of Mails Downloaded	17-19
17.10.6	Unable to Publish and Archive Space Mail	17-20
17.10.7	Changing Passwords on Microsoft Exchange	17-20
17.10.8	Mail Content Sent as Attachments	17-21

18 Managing the People Connections Service

18.1	What You Should Know About the People Connections Service	18-1
18.2	People Connections Prerequisites	18-2
18.3	Setting Up a Proxy Server for Activity Stream	18-2

18.4	Archiving the Activity Stream Schema	18-2
18.5	Configuring Cache Options for the Profile Service	18-3

19 Managing Subscriptions and Notifications

19.1	Setting Up Default Subscription Preferences	19-2
19.1.1	What You Should Know About Subscription Defaults	19-2
19.1.2	Setting Subscription Defaults	19-4
19.1.3	Setting Subscriptions Preferences in Spaces	19-7
19.2	Setting Up Notifications	19-7
19.2.1	What You Should Know About Connection Channels	19-8
19.2.2	Notification Prerequisites	19-8
19.2.2.1	Installation	19-9
19.2.2.2	Configuration	19-9
19.2.2.3	Security	19-9
19.2.2.4	Limitations	19-9
19.2.3	Configuration Roadmap for Notifications	19-10
19.2.4	Specifying the Notifications Channel Using Fusion Middleware Control	19-11
19.2.5	Specifying the Notifications Channel Using WLST	19-12
19.2.6	Example - Setting Up Mail Notifications for the Spaces Application Using WLST	19-12
19.3	Creating and Applying Custom Notification Templates	19-13
19.3.1	What You Should Know About Overwriting Default Notification Templates	19-14
19.3.2	Overwriting a Default Notifications Template	19-17
19.4	Testing the Notifications Connection	19-17
19.5	Troubleshooting Issues with Notifications	19-18

20 Managing Personalization for WebCenter Portal

20.1	What You Should Know About Personalization for WebCenter Portal	20-1
20.2	Before You Begin: Performing Required Configurations	20-2
20.2.1	Introduction	20-2
20.2.2	Configuring an Identity Asserter	20-2
20.2.3	Configuring the WebLogic Server Credential Store	20-2
20.3	Other Personalization Prerequisites	20-2
20.3.1	Personalization Installation Requirements	20-3
20.3.2	Personalization Configuration Requirements	20-3
20.3.3	Personalization Security	20-3
20.3.4	Personalization Limitations	20-4
20.3.5	Personalization Configuration Options	20-4
20.4	Configuring the WebCenter OPSS Trust Service	20-5
20.4.1	Configuring the Trust Service in the WebCenter Portal Domain	20-5
20.4.2	Configuring the Trust Service in the Integrated WLS Domain	20-6
20.4.3	Configuring Cross-Domain Trust	20-7
20.5	Configuring Providers	20-7
20.5.1	Creating or Modifying Provider Connection Settings	20-8
20.5.1.1	Understanding Personalization Connection Information	20-8
20.5.1.2	Connection Configuration Attributes	20-9
20.5.1.3	Configuring Connections Using WLST	20-9

20.5.1.4	Configuring Connections Using JConsole	20-10
20.5.1.4.1	Creating a New Connection Using JConsole	20-10
20.5.1.4.2	Editing Connection Settings Using JConsole	20-10
20.5.1.5	Configuring Connections Using Fusion Middleware Control	20-11
20.5.1.6	Writing a Custom Configuration Class	20-11
20.5.2	Configuring the CMIS Provider	20-11
20.5.3	Configuring the Activity Graph Provider	20-12
20.5.4	Configuring the Oracle People Connections Locator	20-13
20.5.5	Configuring Custom Providers	20-15
20.6	Configuring Coherence	20-15
20.7	Configuring Content Presenter	20-17
20.7.1	Configuring the WebCenter Portal Application's Content Server Connection	20-18
20.7.1.1	Configuring Connections for the Spaces Application Using WLST	20-18
20.7.1.2	Configuring Connections for the Spaces Application Using Fusion Middleware Control	20-18
20.7.2	Configuring the Content Presenter Task Flow Parameters	20-19
20.7.3	Configuring the Conductor's Scenario Tags	20-20
20.8	Configuring Single Sign-on	20-20
20.9	Overriding the Default Security Settings	20-21
20.9.1	Allowing Anonymous Execution of Scenarios	20-21
20.9.2	Disabling Scenario Creation by Anonymous Users	20-21
20.9.3	Disabling Scenario Creation by Authenticated Users	20-22

21 Managing the RSS Service

21.1	What You Should Know About the RSS Service	21-1
21.2	RSS Prerequisites	21-1
21.3	Setting Up a Proxy Server for External RSS News Feeds	21-1
21.4	Testing External RSS News Feed Connections	21-2

22 Managing Oracle SES Search in WebCenter Portal

22.1	What You Should Know About WebCenter Portal's Search with Oracle SES	22-2
22.2	Configuration Roadmaps for Oracle SES in WebCenter Portal	22-3
22.3	Prerequisites for using Oracle SES	22-7
22.3.1	Oracle SES - Installation	22-7
22.3.2	Oracle SES - Configuration	22-8
22.3.3	Oracle SES - Security	22-10
22.4	Setting Up Oracle SES Connections	22-10
22.4.1	Registering Oracle Secure Enterprise Search Servers	22-10
22.4.1.1	Registering Oracle SES Search Connections Using Fusion Middleware Control	22-11
22.4.1.2	Registering Oracle SES Connections Using WLST	22-12
22.4.2	Choosing the Active Oracle SES Connection	22-13
22.4.2.1	Choosing the Active Oracle SES Connection Using Fusion Middleware Control	22-13
22.4.2.2	Choosing the Active Oracle SES Connection Using WLST	22-14
22.4.3	Modifying Oracle SES Connection Details	22-14

22.4.3.1	Modifying Oracle SES Connection Details Using Fusion Middleware Control	22-15
22.4.3.2	Modifying Oracle SES Connection Details Using WLST	22-15
22.4.4	Deleting Oracle SES Connections	22-16
22.4.4.1	Deleting Search Connections Using Fusion Middleware Control	22-16
22.4.4.2	Deleting Search Connections Using WLST	22-16
22.4.5	Testing Oracle SES Connections	22-17
22.5	Configuring Oracle SES to Search Framework Applications	22-17
22.5.1	Setting Up Oracle WebCenter Portal Content Server for Oracle SES Search	22-17
22.5.2	Setting Up Oracle WebCenter Portal's Discussion Server for Oracle SES Search ...	22-22
22.5.3	Setting Up Oracle SES to Search WebCenter Portal	22-23
22.5.3.1	Logging on to the Oracle SES Administration Tool	22-24
22.5.3.2	Setting Up Oracle SES to Search Documents	22-24
22.5.3.3	Setting Up Oracle SES to Search Discussions and Announcements	22-28
22.5.3.4	Additional Oracle SES Configuration	22-33
22.5.4	Setting Up WebCenter Portal: Framework for Oracle SES Search	22-33
22.5.4.1	Configuring Framework Applications After Deployment	22-34
22.5.4.1.1	Modifying Search Parameters Using WLST	22-34
22.5.4.1.2	Configuring Search Crawlers Using WLST	22-34
22.5.4.1.3	Configuring Search Parameters and Crawlers Using Fusion Middleware Control	22-36
22.6	Configuring Oracle SES to Search Spaces Applications	22-37
22.6.1	Setting Up WebCenter Portal: Spaces for Oracle SES Search	22-37
22.6.1.1	Configuring Search Parameters Using WLST	22-42
22.6.1.2	Configuring Search Parameters and Crawlers Using Fusion Middleware Control ..	22-43
22.6.2	Setting Up Oracle WebCenter Portal: Content Server for Oracle SES Search	22-44
22.6.3	Setting Up Oracle WebCenter Portal Discussion Server for Oracle SES Search	22-48
22.6.4	Setting Up Oracle SES to Search WebCenter Portal	22-49
22.6.4.1	Logging on to the Oracle SES Administration Tool	22-50
22.6.4.2	Setting Up Oracle SES to Search Documents	22-50
22.6.4.3	Setting Up Oracle SES to Search Discussions and Announcements	22-54
22.6.4.4	Setting Up Oracle SES to Search Spaces, Lists, Pages, and People	22-59
22.6.4.5	Excluding Services from the Spaces Crawler	22-61
22.6.4.6	Additional Oracle SES Configuration	22-62
22.6.5	Configuring Search Crawlers Using WLST	22-63
22.6.6	Configuring Oracle SES Search for Spaces Using Python Script	22-65
22.6.7	Tips for Crawling Page Contents	22-66
22.7	Troubleshooting Issues with Oracle SES Search	22-66
22.7.1	No Search Results Found	22-66
22.7.1.1	Oracle SES Connection	22-67
22.7.1.2	Documents and Discussions Connections	22-67
22.7.1.3	WebCenter Portal Crawl Configuration	22-67
22.7.1.4	Oracle SES Configuration	22-67
22.7.1.5	User Authentication	22-68
22.7.1.6	Oracle SES Crawling	22-68
22.7.1.7	Oracle SES Authorization	22-68

22.7.2	Search Failure Errors	22-69
22.7.3	Cannot Grant View Permissions to WebCenter Portal	22-69
22.7.4	Restricting Oracle SES Results by Source Group or Source Type	22-69
22.7.5	Search Results Do Not Include Secured Resources	22-70
22.7.6	Search Results Do Not Include Documents	22-71
22.7.7	Search Results Do Not Include Discussions and Announcements	22-71
22.7.8	Search Results Do Not Include Recently Added Resources	22-71
22.7.9	Search Results Do Not Reflect Authorization Changes	22-72
22.7.10	Search Results Do Not Include Resources Available to Wide Audience	22-72

23 Managing the Worklist Service

23.1	Configuration Roadmaps for the Worklist Service	23-1
23.1.1	Roadmap - Configuring the Worklist Service for WebCenter Portal: Spaces	23-2
23.1.2	Roadmap - Configuring the Worklist Service for Framework applications	23-3
23.2	What You Should Know About BPEL Connections	23-5
23.3	BPEL Server Prerequisites	23-6
23.3.1	BPEL Server - Installation and Configuration	23-6
23.3.2	BPEL Server - Security Considerations	23-7
23.3.3	BPEL Server - Limitations in WebCenter Portal	23-7
23.4	Setting Up Worklist Connections	23-7
23.4.1	What You Should Know About Worklist Connections	23-7
23.4.2	Registering Worklist Connections	23-8
23.4.2.1	Registering Worklist Connections Using Fusion Middleware Control	23-8
23.4.2.2	Registering Worklist Connections Using WLST	23-11
23.4.3	Activating a Worklist Connection	23-11
23.4.3.1	Activating a Worklist Connections Using Fusion Middleware Control	23-11
23.4.3.2	Activating a Worklist Connections Using WLST	23-12
23.4.4	Modifying Worklist Connection Details	23-12
23.4.4.1	Modifying Worklist Connection Details Using Fusion Middleware Control ..	23-13
23.4.4.2	Modifying Worklist Connection Details Using WLST	23-13
23.4.5	Deleting Worklist Connections	23-13
23.4.5.1	Deleting Worklist Connections Using Fusion Middleware Control	23-14
23.4.5.2	Deleting Worklist Connections Using WLST	23-14
23.5	Troubleshooting Issues with Worklists	23-15
23.5.1	Unavailability of the Worklist Service Due to Application Configuration Issues ..	23-15
23.5.1.1	adf-config.xml Refers to a Non-Existent BPEL Connection	23-15
23.5.1.2	adf-config.xml Has No Reference to a BPEL Connection	23-16
23.5.1.3	No Rows Yet Message Displays	23-16
23.5.2	Unavailability of the Worklist Service Due to Server Failure	23-17
23.5.2.1	Users Mismatch in Identity Stores	23-18
23.5.2.2	Shared User Directory Does Not Include the weblogic User	23-19
23.5.2.3	Issues with the wsm-pm Application	23-20
23.5.2.4	Clocks are Out of Sync for More Than Five Minutes	23-20
23.5.2.5	Worklist Service Timed Out or is Disabled	23-20

24 Managing Portlet Producers

24.1	What You Should Know About Portlet Producers	24-1
------	--	------

24.2	Registering WSRP Producers	24-2
24.2.1	Registering a WSRP Producer Using Fusion Middleware Control	24-3
24.2.2	Registering a WSRP Producer Using WLST	24-8
24.2.3	Adding a Grant to the Policy Store for a Mapped User Identity	24-8
24.2.4	Registering a WSRP Portlet Producer in WebCenter Portal: Spaces	24-9
24.2.5	Registering a WSRP Portlet Producer in WebCenter Portal: Framework Applications ..	24-9
24.3	Testing WSRP Producer Connections	24-9
24.4	Registering Oracle PDK-Java Producers	24-9
24.4.1	Registering an Oracle PDK-Java Producer Using Fusion Middleware Control	24-10
24.4.2	Registering an Oracle PDK-Java Producer Using WLST	24-12
24.4.3	Registering an Oracle PDK-Java Portlet Producer in WebCenter Portal: Spaces ...	24-12
24.4.4	Registering an Oracle PDK-Java Portlet Producer in WebCenter Portal: Framework Applications	24-12
24.5	Testing Oracle PDK-Java Producer Connections	24-13
24.6	Editing Producer Registration Details	24-13
24.6.1	Editing Producer Registration Details Using Fusion Middleware Control	24-13
24.6.2	Editing Producer Registration Details Using WLST	24-14
24.6.3	Migrating WSRP Producer Metadata to a New WSDL URL	24-14
24.7	Deregistering Producers	24-14
24.7.1	Deregistering Producers Using Fusion Middleware Control	24-15
24.7.2	Deregister Producers Using WLST	24-15
24.7.3	Deregistering Producers in WebCenter Portal: Spaces	24-16
24.7.4	Deregistering Producers in WebCenter Portal: Framework Applications	24-16
24.8	Deploying Portlet Producer Applications	24-16
24.8.1	Understanding Portlet Producer Application Deployment	24-16
24.8.2	Converting a JSR 286 Portlet Producer EAR File into a WSRP EAR File	24-17
24.8.3	Deploying Portlet Producer Applications Using Oracle JDeveloper	24-18
24.8.4	Deploying Portlet Producer Applications Using Fusion Middleware Control	24-18
24.8.5	Deploying Portlet Producer Applications Using Oracle WebLogic Server Administration Console	24-18
24.8.6	Deploying Portlet Producer Applications Using WLST	24-18
24.9	Configuring WebCenter Services Portlets	24-18
24.9.1	Configuring Service Back-End Connections	24-19
24.9.1.1	Configuring the Documents Service Content Repository Connection	24-19
24.9.1.2	Configuring the Worklist Service Connection	24-20
24.9.1.3	Configuring the Discussions and Announcements Services Connection	24-20
24.9.1.4	Configuring the Mail Service Connection	24-20
24.9.2	Configuring Security for WebCenter Services Portlets	24-21
24.9.3	Troubleshooting WebCenter Services Portlets	24-21
24.9.3.1	Rich Text Editor Not Working for Document Manager and Blogs Portlets	24-21
24.9.3.2	Cannot Manage Lists in the Lists Portlet	24-22
24.9.3.3	Portlet Uses Incorrect Time Zone or Date and Time Format	24-22
24.9.3.4	Portlet Displays Remote Portlet Communication Error	24-23
24.10	Troubleshooting Portlet Producer Issues	24-23
24.10.1	Producer Registration Fails for a WebCenter Portal: Framework Application	24-23
24.10.2	Portlet Unavailable: WSM-00101 Exception	24-24

25 Managing Oracle WebCenter Portal's Pagelet Producer

25.1	About the Pagelet Producer	25-1
25.1.1	Key Concepts	25-2
25.1.2	Support for WSRP and Oracle JPDK Portlets	25-3
25.1.3	Support for OpenSocial Gadgets	25-3
25.1.4	Support for Oracle WebCenter Interaction Portlets	25-3
25.2	Registering the Pagelet Producer	25-3
25.2.1	Registering the Pagelet Producer for WebCenter Portal Applications Using Fusion Middleware Control	25-4
25.2.2	Registering the Pagelet Producer for WebCenter Portal Applications Using WLST	25-5
25.2.3	Configuring the Pagelet Producer Service	25-5
25.2.4	Registering Pagelet Producer Using WebCenter Portal: Spaces	25-6
25.3	Configuring Pagelet Producer Settings	25-6
25.3.1	Logging Settings	25-6
25.3.2	Proxy Settings	25-7
25.3.3	Transform Settings	25-8
25.3.4	CSP Settings	25-8
25.3.5	Kerberos Settings	25-8
25.3.6	OpenSocial Settings	25-8
25.4	Creating Resources	25-9
25.4.1	Configuration Pages: Web and CSP Resources	25-11
25.4.1.1	General	25-11
25.4.1.2	CSP	25-12
25.4.1.3	Policy	25-13
25.4.1.4	Autologin	25-13
25.4.1.4.1	Form Login	25-14
25.4.1.4.2	Basic Login and NTLM Login	25-15
25.4.1.4.3	Kerberos Login	25-15
25.4.1.4.4	Authentication Sources	25-15
25.4.1.5	Headers	25-15
25.4.2	Configuration Pages for WSRP/JPDK Resources (WSRP and Oracle JPDK Portlet Producers)	25-17
25.4.2.1	General	25-17
25.4.2.2	Policy	25-17
25.4.3	Configuration Pages for OpenSocial Resources (OpenSocial Gadget Producers)	25-17
25.4.3.1	General	25-18
25.4.3.2	Policy	25-18
25.5	Creating Pagelets	25-18
25.5.1	General	25-19
25.5.2	Preferences	25-19
25.5.3	Parameters	25-20
25.5.4	Clipper	25-21
25.5.5	Documentation	25-21
25.6	Creating Web Injectors	25-22
25.6.1	General	25-22
25.6.2	Content	25-23
25.7	Creating Custom Parsers	25-23

25.8	Creating Hosted Files	25-24
25.9	Registering WSRP and Oracle JPDK Portlet Producers	25-25
25.9.1	Registering WSRP Portlet Producers	25-26
25.9.2	Registering Oracle JPDK Portlet Producers	25-28
25.9.3	Using WSRP and Oracle JPDK Portlets	25-30
25.10	Troubleshooting	25-30

26 Managing External Applications

26.1	What You Should Know About External Applications	26-1
26.2	Registering External Applications	26-3
26.2.1	Registering External Applications Using Fusion Middleware Control	26-4
26.2.2	Registering External Applications Using WLST	26-8
26.2.3	Registering External Applications in the Spaces Application	26-8
26.2.4	Registering External Applications in Framework Applications	26-8
26.3	Modifying External Application Connection Details	26-8
26.3.1	Modifying External Application Connection Using Fusion Middleware Control ...	26-8
26.3.2	Modifying External Application Connection Using WLST	26-9
26.4	Testing External Application Connections	26-9
26.5	Deleting External Application Connections	26-9
26.5.1	Deleting External Application Connections Using Fusion Middleware Control ...	26-10
26.5.2	Deleting External Application Connections Using WLST	26-10
26.5.3	Deleting External Applications Connections in WebCenter Portal: Spaces	26-10
26.5.4	Deleting External Applications Connections in WebCenter Portal: Framework Applications	26-10

27 Managing REST Services

27.1	What You Should Know About REST Services	27-1
27.2	Performing Required Manual Configurations to Enable REST	27-2
27.3	Understanding Security Tokens	27-2
27.4	Configuring a Proxy Server	27-2
27.5	Changing the REST Root Name	27-4
27.6	Using Compression	27-4
27.7	Handling Authentication	27-4

Part V Advanced Systems Administration for Oracle WebCenter Portal

28 Managing WebCenter Portal Application Security

28.1	Introduction to WebCenter Portal Application Security	28-1
28.2	Default Security Configuration	28-4
28.2.1	Administrator Accounts	28-4
28.2.2	Application Roles and Enterprise Roles	28-4
28.2.3	Default Identity and Policy Stores	28-5
28.2.3.1	File-based Credential Store	28-6
28.2.4	Default Policy Store Permissions and Grants	28-6
28.2.4.1	Permission-based Authorization	28-6
28.2.4.2	Role-mapping Based Authorization	28-6

28.2.4.3	Default Policy Store Permissions for Spaces	28-6
28.2.4.4	Default Code-based Grants	28-7
28.2.5	Post-deployment Security Configuration Tasks	28-7
28.3	Troubleshooting Security Configuration Issues	28-9
28.3.1	Spaces Application Does Not Find Users in LDAP Provider	28-9
28.3.2	Space Created with Errors When Logged in as OID User	28-9
28.3.3	Users Cannot Self-Register when Spaces Configured with Active Directory	28-10
28.3.4	User Made Administrator Does Not Have Administrator Privileges	28-10
28.3.5	OmniPortlet Producer Authorization Exception in SSO Environment	28-10
28.3.6	Deploying the SAML SSO-specific Discussions EAR file Produces an Exception ..	28-11
28.3.7	Configuring SAML Single Sign-on Produces 403 Error	28-11

29 Configuring the Identity Store

29.1	Reassociating the Identity Store with an External LDAP Server	29-2
29.2	Tuning the Identity Store for Performance	29-7
29.2.1	Tuning the Identity Store when Using SSL	29-8
29.2.2	Tuning Performance when Using OVD	29-8
29.2.3	Tuning Performance when Using Active Directory	29-9
29.3	Configuring the GUID Attribute for External LDAP Identity Stores	29-9
29.4	Adding Users to the Embedded LDAP Identity Store	29-10
29.4.1	Adding Users to the Identity Store Using the WLS Administration Console	29-11
29.4.2	Adding Users to the Identity Store Using an LDIF File	29-14
29.5	Moving the Administrator Account to an External LDAP Server	29-19
29.5.1	Migrating WebCenter Portal's Discussions Server to Use an External LDAP	29-20
29.5.2	Changing the Administrator Group Name	29-25
29.6	Configuring the Oracle Content Server to Share the Spaces Identity Store LDAP Server	29-29
29.7	Aggregating Multiple Identity Store LDAP Servers Using libOVD	29-29
29.7.1	Configuring libOVD for Identity Stores with Complete User Profiles	29-30
29.7.2	Configuring libOVD for Identity Stores with Partial User Profiles	29-30
29.7.3	Restoring the Single Authenticator	29-32
29.8	Configuring Dynamic Roles for the Spaces Application	29-32
29.8.1	Overview of Configuring Dynamic Roles	29-33
29.8.2	Prerequisites to Configuring Dynamic Roles	29-34
29.8.3	Installing the OVD Plug-in	29-34
29.8.4	Configuring Dynamic Roles	29-35
29.8.4.1	Configuring OES	29-35
29.8.4.2	Configuring the OVD Plug-in	29-43
29.8.4.3	Configuring the Personalization Attributes	29-46
29.8.4.4	Configuring the Spaces Application to Consume Dynamic Roles	29-46
29.9	Configuring Dynamic Groups for the Spaces Application	29-47
29.9.1	Creating a Dynamic Group Using an LDIF File	29-47
29.9.2	Creating a Dynamic Group Using the Oracle Directory Services Manager	29-49
29.10	Configuring the REST Service Identity Asserter	29-49
29.10.1	Understanding the REST Service Instance and Identity Asserter	29-49
29.10.2	Setting up the Client Application	29-50
29.10.3	Configuring the WLS Trust Service Asserter	29-52

30 Configuring the Policy and Credential Store

30.1	Creating a root Node	30-2
30.2	Reassociating the Credential and Policy Store Using Fusion Middleware Control	30-2
30.3	Reassociating the Credential and Policy Store Using WLST	30-4
30.4	Reassociating the Policy and Credential Store with a Database	30-5
30.5	Managing Credentials	30-6
30.6	Managing Users and Application Roles	30-6
30.6.1	Granting the Spaces Administrator Role	30-6
30.6.1.1	Granting the Spaces Administrator Role Using Fusion Middleware Control ...	30-7
30.6.1.2	Granting the Spaces Administrator Role Using WLST	30-9
30.6.2	Granting Application Roles	30-9
30.6.2.1	Granting Application Roles Using Fusion Middleware Control	30-10
30.6.2.2	Granting Application Roles Using WLST	30-12
30.6.3	Using the Runtime Administration Pages	30-12
30.7	Configuring Self-Registration By Invitation in the Spaces Application	30-12
30.8	Setting the Policy Store Refresh Interval and Other Cache Settings	30-13
30.8.1	Setting the Policy Store Refresh Interval	30-13
30.8.2	Setting the Connection Pool Cache	30-13
30.8.3	Setting User Cache Settings	30-14
30.8.4	Setting Group Cache Settings	30-14

31 Configuring Single Sign-on

31.1	Introduction to Single Sign-on	31-1
31.2	Configuring Oracle Access Manager (OAM)	31-2
31.2.1	OAM Components and Topology	31-2
31.2.2	Roadmap to Configuring OAM	31-5
31.2.3	Installing and Configuring OAM	31-7
31.2.3.1	Installing and Configuring OAM 11g	31-7
31.2.3.1.1	Installing and Configuring OAM 11g	31-7
31.2.3.1.2	Installing and Configuring the Oracle HTTP Server	31-8
31.2.3.1.3	Installing the WebGate on the WebTier	31-8
31.2.3.1.4	Registering the WebGate Agent	31-10
31.2.3.2	Installing and Configuring OAM 10g	31-13
31.2.3.2.1	Installing and Configuring OAM 10g	31-13
31.2.3.2.2	Installing and Configuring the Oracle HTTP Server	31-13
31.2.3.2.3	Configuring the WebCenter Portal Policy Domain	31-14
31.2.3.2.4	Installing the WebGate 10g on the WebTier	31-17
31.2.4	Configuring the WebLogic Domain for OAM	31-17
31.2.4.1	Configuring the Oracle Internet Directory Authenticator	31-18
31.2.4.2	Configuring the OAM Identity Asserter	31-22
31.2.4.3	Configuring the Default Authenticator and Provider Order	31-25
31.2.4.4	Adding an OAM Single Sign-on Provider	31-25
31.2.5	Installing and Configuring the Oracle HTTP Server	31-25
31.2.6	Additional Single Sign-on Configurations	31-28
31.2.6.1	Configuring WebCenter Portal: Spaces for SSO	31-29
31.2.6.2	Configuring the Discussions Server for SSO	31-29

31.2.6.2.1	Creating a Discussions Server Connection for Spaces	31-30
31.2.6.3	Configuring the Worklist Service for SSO	31-30
31.2.6.4	Configuring OAM for RSS Feeds Using External Readers	31-30
31.2.6.4.1	Unprotecting RSS Feeds in OAM 11g	31-30
31.2.6.4.2	Unprotecting RSS Feeds in OAM 10g	31-31
31.2.6.5	Configuring the WebLogic Server Administration Console and Enterprise Manager for OAM 10g	31-31
31.2.6.6	Configuring the WebLogic Server Administration Console and Enterprise Manager for OAM 11g	31-33
31.2.6.7	Configuring Secure Enterprise Search for SSO	31-34
31.2.6.8	Configuring Content Server for SSO	31-34
31.2.6.9	Restricting Access with Connection Filters	31-34
31.2.6.10	Configuring Portlet Producers and Additional Components	31-36
31.2.7	Testing Your OAM Installation	31-36
31.3	Configuring Oracle Single Sign-On (OSSO)	31-37
31.3.1	Roadmap to Configuring OSSO	31-37
31.3.2	OSSO Components and Topology	31-38
31.3.3	Configuring the Oracle HTTP Server and Associated Modules	31-39
31.3.4	Configuring the OSSOIdentityAsserter	31-41
31.3.5	Registering OHS with Oracle SSO	31-44
31.3.6	Additional Configurations	31-48
31.3.6.1	Configuring WebCenter Portal: Spaces for SSO	31-49
31.3.6.2	Restricting Access Using the WebTier OHS Ports	31-49
31.3.6.3	Configuring the Discussions Server for SSO	31-49
31.3.6.4	Configuring the Worklist Service for SSO	31-49
31.3.6.5	Configuring Oracle Content Server for SSO	31-49
31.3.6.6	Configuring OSSO for RSS Feeds Using External Readers	31-49
31.3.6.7	Configuring SES Crawl for SSO	31-50
31.4	Configuring SAML-based Single Sign-on	31-50
31.4.1	SAML Components and Topology	31-51
31.4.2	Configuring SAML-based Single Sign-on	31-53
31.4.2.1	SAML Single Sign-on Prerequisites	31-53
31.4.2.1.1	Configuring Oracle Content Server for SAML SSO	31-54
31.4.2.1.2	Configuring the Discussions Server for SAML SSO	31-55
31.4.2.1.3	Configuring and Exporting the Certificates	31-56
31.4.2.1.4	Setting Up SSL	31-57
31.4.2.2	Configuring SAML-based SSO	31-57
31.4.2.2.1	The Single Sign-on Script	31-57
31.4.2.2.2	Using the Scripts	31-62
31.4.2.3	Configuring SAML SSO for RSS Using External Readers	31-65
31.4.2.4	Checking Your Configuration	31-65
31.4.2.5	Disabling Your SAML SSO Configuration	31-66
31.4.2.6	Removing Your SAML SSO Configuration	31-66
31.5	Configuring SSO for Microsoft Clients	31-67
31.5.1	Microsoft Client SSO Concepts	31-68
31.5.2	System Requirements	31-69
31.5.3	Configuring Microsoft Clients	31-69
31.5.3.1	Configuring the Negotiate Identity Assertion Provider	31-71

31.5.3.2	Configuring an Active Directory Authentication Provider	31-73
31.5.3.3	Configuring WebCenter Portal: Spaces	31-78
31.5.3.4	Configuring the Discussions Server for SSO	31-79
31.6	Configuring SSO with Virtual Hosts	31-79
31.6.1	Understanding the Need for a Virtual Host	31-79
31.6.2	Configuring Virtual Hosts for OSSO	31-80
31.6.3	Configuring Virtual Hosts for OAM 10g	31-81
31.6.4	Configuring Virtual Hosts for OAM 11g	31-82
31.6.5	Configuring WebCenter Portal for Virtual Hosts	31-83
31.6.6	Testing Your Configuration	31-83

32 Configuring Framework Applications for Single Sign-on

32.1	Configuration Overview	32-1
32.2	Single Sign-on Prerequisites	32-2
32.2.1	Adding CLIENT-CERT in web.xml	32-2
32.2.2	Setting the Cookie Path for JSESSIONID	32-2
32.2.3	Determining the Public and Protected URIs for Your Application	32-2
32.2.4	Implications of Embedded Login	32-3
32.2.5	Handling Logout	32-3
32.3	Configuring the WebTier	32-4
32.4	Configuring Framework and Portlet Producer Applications for OAM	32-4
32.4.1	Configuring Framework Applications for OAM 10g	32-4
32.4.2	Configuring Portlet Producer Applications for OAM 10g	32-5
32.4.3	Configuring Framework Applications for OAM 11g	32-6
32.4.4	Configuring Portlet Producer Applications for OAM 11g	32-6
32.5	Configuring Framework Applications for OSSO	32-7
32.6	Configuring Framework Applications for SAML SSO	32-7
32.6.1	Configuring SAML SSO for a Destination Framework Application	32-8
32.6.1.1	Enabling the Destination Site	32-9
32.6.1.2	Configuring a Relying Party	32-9
32.6.1.3	Configuring an Asserting Party	32-10
32.6.2	Configuring SAML SSO for a Source Framework Application	32-11
32.6.2.1	Protecting SAML ITS	32-12
32.6.2.2	Setting the Cookie Path for JSESSIONID	32-12
32.6.2.3	Setting the SSO Property to True	32-12
32.6.2.4	Configuring the SAML Credential Mapping Provider	32-13
32.6.2.5	Configuring a Relying Party	32-13
32.6.2.6	Configuring the Source Site Federation Services	32-14
32.6.2.7	Configuring the SAML Identity Assertion Provider	32-15
32.6.2.8	Configuring the Destination Site Federation Services	32-18
32.6.2.9	Configuring Other Destination Applications	32-18

33 Configuring SSL

33.1	Securing the Browser Connection to Spaces with SSL	33-2
33.1.1	Creating the Custom Keystore	33-2
33.1.2	Configuring the Custom Identity and Java Trust Keystores	33-4

33.1.3	Configuring the SSL Connection	33-7
33.2	Securing the Browser Connection to a Framework Application with SSL	33-9
33.3	Securing the Connection from Oracle HTTP Server to Spaces with SSL	33-10
33.3.1	Configuring the Identity and Trust Keystores	33-10
33.3.2	Configuring the SSL Connection	33-10
33.3.3	Installing the Oracle HTTP Server	33-12
33.3.4	Wiring the Spaces Ports to the HTTP Server	33-13
33.3.5	Configuring the SSL Certificates	33-15
33.4	Securing the Browser Connection to the Discussions Service with SSL	33-15
33.4.1	Creating the Custom Keystore	33-15
33.4.2	Configuring the Identity and Trust Key Stores	33-17
33.4.3	Configuring the SSL Connection	33-21
33.5	Securing the Spaces Connection to Portlet Producers with SSL	33-23
33.5.1	Configuring the Identity and Trust Key Stores	33-24
33.5.2	Configuring the SSL Connection	33-27
33.5.3	Registering the SSL-enabled WSRP Producer and Running the Portlets	33-28
33.5.4	Registering the SSL-enabled PDK-Java Producer and Running the Portlets	33-29
33.6	Securing the Spaces Connection to the LDAP Identity Store	33-31
33.6.1	Exporting the OID Certificate Authority (CA)	33-32
33.6.2	Setting Up the WebLogic Server	33-32
33.7	Securing the Spaces Connection to Content Server with SSL	33-32
33.7.1	Configuring a Keystore and Key on the Client Side	33-32
33.7.2	Configuring a Keystore and Key on the Server Side	33-33
33.7.3	Verifying Signatures of Trusted Clients	33-33
33.7.4	Securing Identity Propagation	33-34
33.8	Securing the Spaces Connection to IMAP and SMTP with SSL	33-35
33.9	Securing a Framework Application's Connection to IMAP and SMTP with SSL	33-36
33.10	Securing the Connection to Oracle SES with SSL	33-36
33.11	Securing the Spaces Connection to Microsoft Live Communication Server and Office Communication Server with SSL	33-37
33.12	Securing the Spaces Connection to an External BPEL Server with SSL	33-37

34 Configuring WS-Security

34.1	Configuring WS-Security for a Simple Topology	34-1
34.1.1	Roadmap to Configuring WS-Security for a Simple Topology	34-2
34.1.2	Setting Up the WebCenter Portal Domain Keystore	34-3
34.1.2.1	Creating the WebCenter Portal Domain Keystore	34-3
34.1.2.2	Configuring the Keystore with WLST	34-5
34.1.2.3	Configuring the Keystore Using Fusion Middleware Control	34-6
34.1.3	Configuring the Discussions Server for a Simple Topology	34-7
34.1.3.1	Securing the Discussions Service End Points	34-8
34.1.3.1.1	Securing the Discussions Server End Points Using Fusion Middleware Control	34-8
34.1.3.1.2	Securing the Discussions Server End Points Using WLST	34-11
34.1.3.2	Configuring the Discussions Server Connection Settings	34-12
34.1.4	Command Summary for a Simple Topology	34-12
34.2	Configuring WS-Security for a Typical Topology	34-13

34.2.1	Roadmap to Configuring WS-Security for a Typical Topology	34-14
34.2.2	Setting Up the WebCenter Portal Domain Keystore	34-14
34.2.2.1	Creating the WebCenter Portal Domain Keystore	34-14
34.2.2.2	Configuring the Keystore Using WLST	34-16
34.2.2.3	Configuring the Keystore Using Fusion Middleware Control	34-17
34.2.3	Configuring the Discussions Server for a Typical Topology	34-18
34.2.4	Setting Up the SOA Domain	34-18
34.2.4.1	Creating the SOA Domain Keystore	34-18
34.2.4.2	Configuring the Keystore Using WLST	34-20
34.2.4.3	Configuring the Keystore Using Fusion Middleware Control	34-20
34.2.5	Command Summary for a Typical Topology	34-21
34.3	Configuring WS-Security for a Complex Topology	34-23
34.3.1	Roadmap to Configuring WS-Security for a Complex Topology	34-24
34.3.2	Setting Up the WebCenter Portal Domain Keystores	34-25
34.3.2.1	Creating the WebCenter Portal Domain Keystores	34-25
34.3.2.2	Configuring the Keystore Using WLST	34-27
34.3.2.3	Configuring the Keystore Using Fusion Middleware Control	34-28
34.3.3	Configuring the Discussions Server for a Complex Topology	34-29
34.3.3.1	Securing the Discussions Service End Points	34-30
34.3.3.2	Creating the Discussions Server Keystore	34-30
34.3.3.3	Updating the Credential Store	34-31
34.3.3.4	Configuring the Discussions Server Connection Settings	34-32
34.3.4	Setting Up the First SOA Domain	34-32
34.3.4.1	Creating the SOA Domain Keystore	34-32
34.3.4.2	Configuring the Keystore Using WLST	34-34
34.3.4.3	Configuring the Keystore Using Fusion Middleware Control	34-35
34.3.5	Setting Up the Second SOA Domain	34-36
34.3.5.1	Creating the SOA Domain Keystore	34-36
34.3.5.2	Configuring the Keystore Using WLST	34-38
34.3.5.3	Configuring the Keystore Using Fusion Middleware Control	34-39
34.3.5.4	Configuring the Spaces Worklist Connection for the Second SOA Server	34-40
34.3.6	Setting Up the External Portlet Domain Keystore	34-41
34.3.6.1	Creating the External Portlet Domain Keystore	34-42
34.3.6.2	Configuring the Keystore Using WLST	34-43
34.3.6.3	Configuring the Keystore Using Fusion Middleware Control	34-44
34.3.7	Setting Up the External WebCenter Portal Domain Keystore	34-45
34.3.7.1	Creating the External WebCenter Portal Domain Keystore	34-45
34.3.7.2	Configuring the Keystore Using WLST	34-46
34.3.7.3	Configuring the Keystore Using Fusion Middleware Control	34-47
34.3.8	Command Summary for a Complex Topology	34-48
34.4	Securing Spaces for Applications Consuming Spaces Client APIs with WS-Security ..	34-52
34.4.1	Configuring a Simple Topology for Applications Consuming Spaces Client APIs	34-52
34.4.2	Configuring a Typical Topology for Applications Consuming Spaces Client APIs	34-52
34.4.3	Configuring a Complex Topology for Applications Consuming Spaces Client APIs	34-53

35 Configuring Security for Portlet Producers

35.1	Securing a WSRP Producer	35-1
35.1.1	Deploying the Producer	35-1
35.1.2	Attaching a Policy to the Producer Endpoint	35-1
35.1.3	Setting Up the Keystores	35-6
35.2	Securing a PDK-Java Producer	35-6
35.2.1	Defining a Shared Key as a Password Credential	35-7
35.2.1.1	Defining a Shared Key Using Fusion Middleware Control	35-7
35.2.1.2	Defining a Shared Key Using WLST	35-8

36 Using WebCenter Portal Administration Console

36.1	Introduction to WebCenter Portal Administration Console	36-1
36.2	Accessing the WebCenter Portal Administration Console	36-2
36.3	Configuring Application Defaults	36-2
36.3.1	Choosing a Default Page Template	36-3
36.3.2	Choosing Default Resource Catalogs	36-3
36.3.3	Choosing a Default Navigation	36-4
36.3.4	Choosing a Default Skin	36-4
36.3.5	Choosing the Default Base Resource URL	36-5
36.4	Managing Application Members and Roles	36-5
36.4.1	Understanding Users	36-6
36.4.2	Understanding Application Roles and Permissions	36-6
36.4.2.1	Understanding Application Roles	36-6
36.4.2.1.1	Default Application Roles	36-6
36.4.2.1.2	Custom Application Roles	36-7
36.4.2.2	Understanding Application Permissions	36-7
36.4.2.2.1	Application Permissions	36-8
36.4.2.2.2	Discussion Server Role Mapping	36-10
36.4.2.2.3	Understanding Enterprise Group Role Mapping	36-11
36.4.3	Managing Users	36-11
36.4.3.1	Adding Members to Application Roles	36-11
36.4.3.2	Assigning a User to a Different Role	36-13
36.4.3.3	Giving a User Administrative Privileges	36-14
36.4.3.4	Revoking Application Roles	36-14
36.4.3.5	Adding or Removing Users	36-14
36.4.4	Managing Application Roles and Permissions	36-14
36.4.4.1	Defining Application Roles	36-15
36.4.4.2	Modifying Application Role Permissions	36-16
36.4.4.3	Granting or Removing Roles for Unauthenticated Users	36-17
36.4.4.4	Granting Roles to All Authenticated Users	36-18
36.4.4.5	Deleting Application Roles	36-18
36.5	Managing Application Resources	36-19
36.5.1	Working with Pages	36-20
36.5.1.1	Creating a Page	36-20
36.5.1.2	Creating a Sub Page	36-22
36.5.1.3	Setting Page Access	36-22
36.5.1.3.1	Setting Permissions on an Individual Page	36-23

36.5.1.3.2	Setting Permissions on the Root Node	36-25
36.5.1.4	Reordering a Page	36-25
36.5.1.5	Moving a Page in the Page Hierarchy	36-26
36.5.1.6	Renaming a Page	36-26
36.5.2	Creating a Resource	36-27
36.5.3	Copying a Resource	36-28
36.5.4	Editing Resources	36-28
36.5.4.1	Editing the Source Code of a Resource	36-28
36.5.4.2	Editing a Resource by Using the Edit Dialog	36-29
36.5.5	Setting Properties on a Resource	36-30
36.5.5.1	Accessing the Edit Properties Dialog of a Resource	36-30
36.5.5.2	Renaming, Describing, and Categorizing a Resource	36-31
36.5.5.3	Associating an Icon with a Resource	36-32
36.5.5.4	Working with Attributes of a Resource	36-32
36.5.5.4.1	Associating an Attribute with a Resource	36-32
36.5.5.4.2	Deleting an Attribute of a Resource	36-33
36.5.6	Showing or Hiding a Resource	36-33
36.5.7	Setting Resource Security	36-34
36.5.8	Downloading and Uploading a Resource	36-35
36.5.9	Previewing a Resource	36-36
36.5.10	Deleting a Resource	36-37
36.6	Managing Services, Portlet Producers, and External Applications	36-37
36.6.1	Managing Content	36-38
36.6.1.1	Creating a New Folder	36-39
36.6.1.2	Creating a Wiki Page	36-39
36.6.1.3	Editing a File	36-39
36.6.1.4	Uploading a Document	36-40
36.6.1.5	Checking Out a Document	36-40
36.6.1.6	Uploading a New Version of a Document	36-41
36.6.1.7	Viewing Version History of a Content Item	36-41
36.6.1.8	Getting Direct and Download URLs of a Document	36-42
36.6.1.9	Organizing Columns for the Displayed Content	36-42
36.6.1.9.1	Showing Columns	36-42
36.6.1.9.2	Reordering Columns	36-43
36.6.1.10	Setting Up Security on Folders and Documents	36-43
36.6.2	Managing Portlet Producers	36-44
36.6.2.1	Registering Portlet Producers	36-44
36.6.2.2	Editing and Deleting Portlet Producers	36-45
36.6.3	Managing External Applications	36-45
36.6.3.1	Registering External Applications	36-46
36.6.3.2	Editing and Deleting External Applications	36-47
36.6.4	Creating and Configuring Polls	36-47
36.6.4.1	What You Should Know About the Polls Service	36-47
36.6.4.2	Creating, Configuring, and Analyzing a Poll	36-48

37 Managing a Multilanguage Portal

37.1	What You Should Know About Languages in the Spaces Application	37-1
------	--	------

37.1.1	Languages Supported Out-of-the-Box by Spaces	37-2
37.2	Limiting Edits to a Particular String or Space	37-3
37.2.1	Finding the Resource Key for a String	37-3
37.2.2	Finding the GUID for a Space	37-4
37.3	Modifying Strings	37-5
37.4	Adding Support to Spaces for a New Language	37-7
37.5	Presenting Translated Content Through a Content Presenter Template	37-9

38 Monitoring Oracle WebCenter Portal Performance

38.1	Understanding Oracle WebCenter Portal Performance Metrics.....	38-1
38.1.1	WebCenter Portal Metric Collection: Recent History and Since Startup	38-2
38.1.2	Common WebCenter Portal Metrics	38-3
38.1.3	Common WebCenter Portal Performance Issues and Actions	38-8
38.1.4	WebCenter Portal Service-Specific Metrics	38-8
38.1.4.1	Announcement Metrics	38-9
38.1.4.2	BPEL Worklist Metrics	38-10
38.1.4.3	Content Repository Metrics	38-11
38.1.4.4	Discussion Metrics	38-16
38.1.4.5	Events Metrics	38-18
38.1.4.6	External Application Metrics	38-20
38.1.4.7	Instant Messaging and Presence (IMP) Metrics	38-22
38.1.4.8	Import and Export Metrics	38-23
38.1.4.9	List Metrics	38-23
38.1.4.10	Mail Metrics	38-25
38.1.4.11	Note Metrics	38-27
38.1.4.12	Page Metrics	38-28
38.1.4.13	Portlet Producer Metrics	38-29
38.1.4.14	Portlet Metrics	38-31
38.1.4.15	People Connection Metrics	38-35
38.1.4.16	Poll Metrics	38-36
38.1.4.17	RSS News Feed Metrics	38-37
38.1.4.18	Recent Activity Metrics	38-38
38.1.4.19	Search Metrics	38-38
38.1.5	WebCenter Portal Service-Specific Performance Issues and Actions	38-39
38.1.5.1	Announcements Service	38-40
38.1.5.2	BPEL Worklist Service	38-40
38.1.5.3	Content Repository (Documents and Content Presenter) Service	38-40
38.1.5.4	Discussions Service	38-40
38.1.5.5	External Applications Service	38-41
38.1.5.6	Events Service	38-41
38.1.5.7	Instant Messaging and Presence (IMP) Service	38-41
38.1.5.8	Import and Export	38-41
38.1.5.9	Lists Service	38-41
38.1.5.10	Mail Service	38-42
38.1.5.11	Notes Service	38-42
38.1.5.12	Page Service	38-42
38.1.5.13	Portlets and Producers	38-42

38.1.5.14	People Connections Service	38-42
38.1.5.15	Polls Service	38-43
38.1.5.16	RSS Service	38-43
38.1.5.17	Recent Activities Service	38-43
38.1.5.18	Search Service	38-43
38.1.6	Space Metrics	38-44
38.1.7	Page Metrics	38-45
38.2	Viewing Performance Information	38-48
38.2.1	Monitoring a Spaces Applications	38-48
38.2.1.1	Monitoring Service Metrics	38-49
38.2.1.2	Monitoring Space Metrics	38-49
38.2.1.3	Monitoring Page Metrics for the Spaces Application	38-50
38.2.1.4	Monitoring All Metrics Through the Metrics Palette	38-51
38.2.2	Monitoring Framework Applications	38-52
38.2.2.1	Monitoring Service Metrics	38-52
38.2.2.2	Monitoring Page Metrics for Framework Applications	38-53
38.2.2.3	Monitoring All Metrics Through the Metrics Palette	38-53
38.3	Viewing and Configuring Log Information	38-54
38.3.1	Spaces Application Logs	38-55
38.3.2	Framework Application Logs	38-55

39 Managing Export, Import, Backup, and Recovery of WebCenter Portal

39.1	Exporting and Importing a Spaces Application for Data Migration	39-1
39.1.1	Understanding Spaces Export and Import	39-2
39.1.2	Prerequisites for Spaces Application Export and Import	39-4
39.1.3	Migrating Back-end Components for an Entire Spaces Application	39-4
39.1.3.1	Exporting the LDAP Identity Store	39-5
39.1.3.2	Importing the LDAP Identity Store	39-6
39.1.3.3	Exporting and Importing the LDAP Credential Store	39-6
39.1.3.4	Exporting and Importing the LDAP Policy Store	39-8
39.1.3.5	Exporting and Importing a File-based Credential Store	39-10
39.1.3.6	Exporting and Importing a File-based Policy Store	39-12
39.1.3.7	Exporting Discussions Server Data	39-13
39.1.3.8	Importing Discussions Server Data	39-13
39.1.3.9	Exporting Oracle Content Server Data	39-15
39.1.3.10	Importing Oracle Content Server Data	39-16
39.1.3.11	Exporting Oracle WebLogic Communications Server	39-17
39.1.3.12	Importing Oracle WebLogic Communications Server	39-17
39.1.3.13	Exporting Portlet Producers	39-18
39.1.3.14	Importing Portlet Producers	39-18
39.1.4	Exporting an Entire Spaces Application	39-18
39.1.4.1	Exporting the Spaces Application Using Fusion Middleware Control	39-19
39.1.4.2	Exporting the Spaces Application Using WLST	39-22
39.1.5	Importing an Entire Spaces Application	39-22
39.1.5.1	Importing a Spaces Application Using Fusion Middleware Control	39-23
39.1.5.2	Importing a Spaces Application Using WLST	39-24
39.1.5.3	Verify an Imported Spaces Application	39-24

39.1.6	Prerequisites for Individual Space Export and Import	39-24
39.1.7	Migrating Back-end Components for Individual Spaces	39-24
39.1.7.1	Exporting Discussions for a Space	39-25
39.1.7.2	Importing Discussions for a Space	39-27
39.1.7.3	Exporting Documents for a Space	39-29
39.1.7.4	Importing Documents for a Space	39-29
39.1.7.5	Exporting/Importing Space Documents using the Document Migration Utility	39-30
39.1.7.5.1	Properties Required to Run the Document Migration Utility	39-31
39.1.7.5.2	Migrating Content Using the Document Migration Utility	39-32
39.1.7.5.3	Running the Document Migration Utility with Additional Logging	39-35
39.1.8	Exporting Individual Spaces	39-36
39.1.8.1	Exporting Individual Spaces Using the Spaces Application	39-36
39.1.8.2	Exporting Individual Spaces Using WLST	39-36
39.1.9	Importing Individual Spaces	39-37
39.1.9.1	Importing Individual Spaces Using the Spaces Application	39-37
39.1.9.2	Importing Individual Spaces Using WLST	39-37
39.1.10	Migrating Back-end Components for Space Templates	39-38
39.1.11	Exporting Space Templates	39-38
39.1.11.1	Exporting Space Templates Using the Spaces Application	39-38
39.1.11.2	Exporting Space Templates Using WLST	39-38
39.1.12	Importing Space Templates	39-39
39.1.12.1	Importing Space Templates Using the Spaces Application	39-39
39.1.12.2	Importing Space Templates Using WLST	39-39
39.1.13	Exporting Spaces Resources	39-39
39.1.13.1	Exporting WebCenter Resources Using the Spaces Application	39-40
39.1.13.2	Exporting WebCenter Resources Using WLST	39-40
39.1.14	Importing Space Resources	39-40
39.1.14.1	Importing WebCenter Resources Using the Spaces Application	39-41
39.1.14.2	Importing WebCenter Resources Using WLST	39-41
39.2	Exporting and Importing Framework Applications for Data Migration	39-41
39.2.1	Understanding Framework Application Export and Import	39-41
39.2.2	Prerequisites for Framework Application Export and Import	39-42
39.2.3	Exporting Portlet Client Metadata (Framework Applications)	39-43
39.2.4	Importing Portlet Client Metadata (Framework Applications)	39-43
39.2.5	Exporting WebCenter Portal Resources (Framework Applications)	39-44
39.2.6	Importing WebCenter Portal Resources (Framework Applications)	39-44
39.2.7	Exporting WebCenter Portal Service Metadata and Data (Framework Applications)	39-45
39.2.8	Importing WebCenter Portal Service Metadata and Data (Framework Applications)	39-47
39.2.9	Migrating Security for WebCenter Portal Applications	39-48
39.2.10	Migrating Data (WebCenter Portal Applications)	39-48
39.2.10.1	Exporting Data (WebCenter Portal Applications)	39-48
39.2.10.2	Importing Data (WebCenter Portal Applications)	39-49
39.3	Migrating Wiki Documents from Other Wiki Applications	39-49
39.3.1	Understanding Document Content in Spaces and Space Templates	39-49
39.3.1.1	Understanding Spaces	39-50

39.3.1.2	Understanding Space Templates	39-50
39.3.1.3	Understanding Folder and File Limitations for a Folder	39-50
39.3.1.4	Understanding Export/Import for Spaces and Space Templates	39-51
39.3.2	Understanding Wiki Documents and Wiki Pages	39-51
39.3.2.1	Understanding Wiki Documents	39-51
39.3.2.2	Understanding Wiki Pages	39-52
39.3.3	Understanding the Document Migration Utility	39-53
39.3.3.1	Understanding the Document Migration Utility's Export Function	39-53
39.3.3.2	Understanding the Document Migration Utility's Import Function	39-54
39.3.3.2.1	Understanding How the Document Migration Utility Handles Metadata	39-55
39.3.3.2.2	Document Migration Archive	39-56
39.3.4	Migrating Data from the Source Wiki Application to Spaces	39-65
39.3.4.1	Preparing WebCenter Portal: Spaces for Importing Wiki Content	39-66
39.3.4.2	Writing and Running a Custom Wiki Extraction Tool to Extract Content from the Wiki Application	39-66
39.3.4.2.1	Extracting and Arranging the Wiki Content	39-67
39.3.4.2.2	Cleaning Up the Source HTML of Wiki Documents	39-68
39.3.4.2.3	Rewriting the URLs	39-68
39.3.4.2.4	Building the ExportImportData.xml Documents	39-70
39.3.4.2.5	Building the Archive File	39-71
39.3.4.3	Using the Document Migration Utility to Import the Archive into the Target Space	39-71
39.3.4.4	Creating Wiki Pages in Spaces for the Content in Content Server	39-72
39.4	Backing Up and Recovering WebCenter Portal Applications	39-72
39.5	Troubleshooting Import and Export Issues for Spaces	39-72
39.5.1	ResourceLimitException Issue	39-73
39.5.2	Spaces and Space Templates Not Available After Import	39-73
39.5.3	Exporting and Importing Spaces in Multibyte Languages	39-73
39.5.4	Page or Space Not Found Messages After Import	39-74
39.5.5	Space Import Archive Exceeds Maximum Upload File Size	39-74
39.5.6	Lists Not Imported Properly	39-74
39.5.7	Importing Spaces Customizations	39-74
39.5.8	Exporting and Importing Spaces with Services Configured	39-78

Part VI Appendixes

A WebCenter Portal Configuration

A.1	Configuration Files	A-1
A.1.1	adf-config.xml and connections.xml	A-2
A.1.2	web.xml	A-5
A.1.2.1	Editing web.xml Properties for Spaces	A-5
A.1.2.2	Editing web.xml Properties for WebCenter Portal Applications	A-6
A.1.3	webcenter-config.xml	A-6
A.2	Cluster Configuration	A-7
A.3	Configuration Tools	A-8
A.4	Tuning Oracle WebCenter Portal Performance	A-9

A.5	Troubleshooting WebCenter Portal Application Configuration Issues	A-10
A.5.1	WebCenter Portal Does Not Display in the Application Deployment Menu in Fusion Middleware Control	A-10
A.5.2	Configuration Options Unavailable	A-12
A.5.3	Configuration Performed in One Application Reflects in Another	A-12
A.5.4	Spaces Application Logs Indicate Too Many Open Files	A-13
A.6	Troubleshooting WLST Command Issues	A-13
A.6.1	None of the WebCenter Portal WLST Commands Work	A-13
A.6.2	WLST Commands Do Not Work for a Particular Service	A-14
A.6.3	A Connection with the Name Connection_Name Already Exists	A-15
A.6.4	WLST Shell is Not Connected to the Oracle WebLogic Managed Server Instance ..	A-15
A.6.5	Application with the Same Name Already Exists in a Domain	A-15
A.6.6	Application with the Same Name Already Exists on a Managed Server	A-16
A.6.7	Already in Domain Runtime Tree Message Displays	A-16

B Oracle HTTP Server Configuration for WebCenter Portal

Glossary

Index

Preface

Welcome to the Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal! This guide describes how to administer Oracle WebCenter Portal, WebCenter Portal: Spaces, and other application deployments built using WebCenter Portal: Framework.

The Guide describes how to start and stop WebCenter Portal applications, how to configure WebCenter Portal components, back-end services, and security, and also how to back up, recover, and migrate WebCenter Portal applications and services.

Audience

This document is intended for:

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

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

Documentation Accessibility

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

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit

<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Related Documents

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

- *Oracle Fusion Middleware Administrator's Guide*
- *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Portal*

- *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*
- *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*
- *Oracle Fusion Middleware Tutorial for Oracle WebCenter Portal Developers*

Conventions

The following text conventions are used in this document:

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

What's New

What's new in Release 11.1.1.6? Faster performance, simplified connection interfaces, and enhanced design-time experience to name a few. Read this quick-reference page for a concise summary of what's new in this release and for pointers to more detailed information.

Note: Patching involves copying a small collection of files over an existing installation. A patch is normally associated with a particular version of an Oracle product and involves updating from one minor version of the product to a newer minor version of the same product (for example, from version 11.1.1.5.0 to version 11.1.1.6.0).

A *patch set* is a single patch that contains a collection of patches designed to be applied together.

All users must move to Release 11.1.1.6.0 for continued support.

New Features for Release 11.1.1.6

The following table lists and describes new features in this release and provides links to more detailed information in our guides.

Feature	Description	For More Information, See...
Blogs	<p>More special characters allowed in blog names:</p> <ul style="list-style-type: none">When you create a blog, you can now use the following special characters in blog names in addition to letters and numbers: ? \ / : [] * ' " <p>Enhanced commenting:</p> <ul style="list-style-type: none">Commenting is now available when you view the list of blog entries and not on just the entry itself.	<ul style="list-style-type: none">"Working with Blogs," in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces</i>

Feature	Description	For More Information, See...
Certification	<p>More technologies certified against the WebCenter Portal application platform:</p> <ul style="list-style-type: none"> ■ Microsoft Lync 2010 for IMP ■ WebSphere Application Server V7 ■ Internet Explorer 9 Browser ■ Chrome Browser 10 and chrome support ■ Microsoft Office 2010 on Windows XP (32-bit and 64 bit) 	<ul style="list-style-type: none"> ■ Section 16.2.3, "Microsoft Lync Prerequisites" ■ Oracle Fusion Middleware Supported System Configurations page at http://www.oracle.com/technology/software/products/ias/files/fusion_certification.html. ■ "Working with Microsoft Office and Explorer Integration," in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces</i>
Discussions service	<ul style="list-style-type: none"> ■ Discussions task flows are streamlined for greater ease of use. 	<ul style="list-style-type: none"> ■ "Working with the Discussions Service," in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces</i>
Documents service	<ul style="list-style-type: none"> ■ Follow a clearer set of steps to connect to the Oracle WebCenter Content repository. ■ Upload multiple files from your desktop by drag and drop. ■ Select and upload multiple files from the Document Explorer in one step. ■ View file upload progress. ■ Share documents more easily. ■ Perform in-context workflow approval. Approver can view and approve or reject unreleased content from the contribution mode without needing to enter edit mode. ■ Enter contribution approval mode on a page with content (either HTML or Site Studio) in a workflow. View and approve or reject unreleased content from contribution approval mode without entering edit mode. 	<ul style="list-style-type: none"> ■ Chapter 11, "Managing Content Repositories" ■ Section 24.9.1.1, "Configuring the Documents Service Content Repository Connection" ■ "Uploading New Files," in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces</i> ■ "Working with the Documents Service Task Flows and Document Components," in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces</i> ■ "Publishing Content Using Content Presenter," in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces</i> ■ "Approving or Rejecting a File in a Workflow," in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces</i>
Events service	<ul style="list-style-type: none"> ■ Task flows are streamlined to enhance usability. For example, users can now view links to events from both calendar and list views. 	<ul style="list-style-type: none"> ■ "Working with the Events Service," in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces</i>
Notifications	<ul style="list-style-type: none"> ■ Subscription messages now use IMP rather than iCal for notifications about events. Consequently, event notifications are added automatically to your Outlook Calendar, without your having to open the notification attachment and add it yourself. 	<ul style="list-style-type: none"> ■ "Subscribing to Events," in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces</i>

Feature	Description	For More Information, See...
Pagelet Producer	<p>More robust Pagelet Producer:</p> <ul style="list-style-type: none"> ■ Use SharePoint web parts, including those requiring Kerberos authentication. ■ Includes support for logging of HTTP traffic between a proxy and a resource. ■ Added detailed pagelet debug logging. ■ Available as a unified producer for non-standards-compliant web applications. ■ Enables consumption of gadgets from other OpenSocial containers, such as iGoogle, and exposure of them as pagelets that can be consumed by WebCenter Portal sites, other Oracle portals, or Oracle Web Content Management for WebCenter sites. ■ Enables production of OpenSocial gadgets and exposure of all existing pagelets as gadgets. 	<ul style="list-style-type: none"> ■ "Creating Pagelets with Oracle WebCenter Portal's Pagelet Producer," in <i>Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal</i> ■ Chapter 25, "Managing Oracle WebCenter Portal's Pagelet Producer"
Pages	<ul style="list-style-type: none"> ■ New Administrator-level Delete Personalization option enables removal of all users' customizations from business role pages or personal pages in one step. ■ New system pages are available to support viewing and managing application metrics, space memberships, spaces, and space templates. ■ The Subscribe system page is now named Self-Service Membership to more-closely reflect its use case. 	<ul style="list-style-type: none"> ■ "Removing All User Customizations from a Business Role Page," in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces</i> ■ "Removing All User Customizations from a Personal Page," in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces</i> ■ "Working with System Pages," in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces</i>
Performance	<p>Accelerated performance at design time and runtime:</p> <ul style="list-style-type: none"> ■ Experience faster initial page downloads. ■ Realize faster creation times for WebCenter Portal: Framework applications. 	

Feature	Description	For More Information, See...
Portlet producers	<ul style="list-style-type: none"> ■ New Enterprise 2.0 portlet producer is available for exposing task flows from WebCenter Portal services as portlets. Integrate portlets with WebCenter Portal applications, Oracle WebLogic Portal, and Oracle WebCenter Interaction. <p>The new Enterprise 2.0 portlet producer is certified with WebSphere, MySQL, Internet Explorer 9, and Chrome 10.</p>	<ul style="list-style-type: none"> ■ "Overview of Portlets," in <i>Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal</i> ■ "Consuming E2.0 Portlet Producer Portlets," in <i>Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal</i> ■ Section 24.9, "Configuring WebCenter Services Portlets"
Publisher	<ul style="list-style-type: none"> ■ Upload multiple files at once through the Publisher task flow. 	<ul style="list-style-type: none"> ■ "Sharing Files Through the Publisher Task Flow," in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces</i>
Search service	<ul style="list-style-type: none"> ■ There are more task flow parameters to limit the scope of searches. Administrators can narrow the scope of searches to specific spaces, services, and document types. They also can add attributes to the list of standard attributes returned with each search result item, and they can hide standard refiners available to users with search results. ■ You can now build portals using a navigation model that enables SES and public search engines, such as Google and Bing, to crawl and index the full text content of pages. 	<ul style="list-style-type: none"> ■ "Working with the Search Service," in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces</i> ■ "Building a Navigation Model for Your Portal," in <i>Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal</i> ■ "Integrating the Search Service," in <i>Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal</i> ■ Chapter 22, "Managing Oracle SES Search in WebCenter Portal"
Security	<ul style="list-style-type: none"> ■ Support is available for dynamically determining group membership via integration with Oracle Entitlements Server 10g. 	<ul style="list-style-type: none"> ■ "Securing Your WebCenter Portal: Framework Application," in <i>Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal</i> ■ Chapter 28, "Managing WebCenter Portal Application Security" ■ "Understanding Security," in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces</i>

Feature	Description	For More Information, See...
Tags service	<ul style="list-style-type: none"> ■ We have updated the edit tags user interface in the Document Explorer task flow. ■ The Tags button component and the Edit Tags task flow have a new parameter that enables developers to disable the Shared control. ■ The previously-named "Tag Cloud" task flow is now called the "Tag Selection" task flow; and a new standalone Tag Cloud task flow is available in the design-time catalog. 	<ul style="list-style-type: none"> ■ "Working with the Tags Service," in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces</i> ■ "Integrating the Tags Service," in <i>Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal</i>
Wikis	<ul style="list-style-type: none"> ■ Access wiki creation features with greater ease: Use a New Wiki Document button in a Documents service task flow or in the wiki itself. ■ Experience improved performance in loading wikis, launching the wiki editor, and saving changes to your wiki. 	<ul style="list-style-type: none"> ■ "Creating a Wiki Document Using the New Wiki Document Action," in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces</i>

Part I

Understanding Oracle WebCenter Portal

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

Part I contains the following chapter:

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

Introduction to Oracle WebCenter Portal Administration

Welcome to Oracle WebCenter Portal!

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

- [Section 1.1, "Introducing Oracle WebCenter Portal"](#)
- [Section 1.2, "Oracle WebCenter Portal Architecture"](#)
- [Section 1.3, "Oracle WebCenter Portal Topology"](#)
- [Section 1.4, "Spaces Application"](#)
- [Section 1.5, "Framework Applications"](#)
- [Section 1.6, "Planning WebCenter Portal Installations"](#)
- [Section 1.7, "Understanding the WebCenter Portal 11g Installation"](#)
- [Section 1.8, "Understanding Administrative Operations, Roles, and Tools"](#)
- [Section 1.9, "Performance Monitoring and Diagnostics"](#)
- [Section 1.11, "WebCenter Portal Application Deployment"](#)
- [Section 1.12, "Data Migration, Backup, and Recovery"](#)
- [Section 1.13, "Oracle WebCenter Portal Administration Tools"](#)

Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal is written specifically for Oracle WebLogic Server—the primary platform for Oracle Fusion Middleware software components such as Oracle WebCenter Portal.

1.1 Introducing Oracle WebCenter Portal

Oracle WebCenter Portal 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 Portal 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 Portal also provides an out-of-the-box enterprise-ready customizable application called *Spaces*,

with a configurable work environment that enables individuals and groups to work and collaborate more effectively.

Oracle WebCenter Portal provides an open and extensible solution that allows users to interact directly with services like instant messaging, documents, content management, discussion forums, wikis, blogs, 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 Portal components and architecture in the following sections:

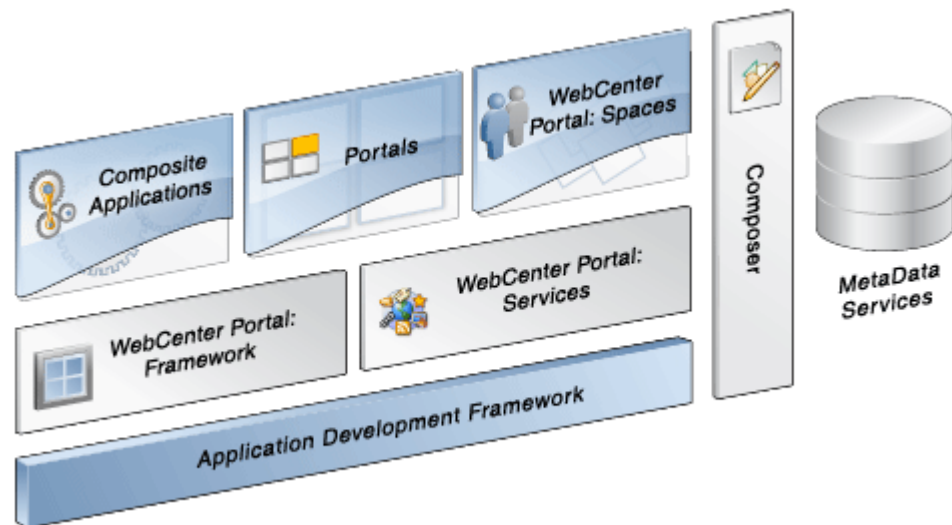
- [Section 1.2, "Oracle WebCenter Portal Architecture"](#)
- [Section 1.3, "Oracle WebCenter Portal Topology"](#)
- [Section 1.4, "Spaces Application"](#)
- [Section 1.5, "Framework Applications"](#)

1.2 Oracle WebCenter Portal Architecture

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

- [WebCenter Portal: Framework](#)
- [Application Development Framework](#)
- [WebCenter Portal: Spaces](#)
- [WebCenter Portal: Services](#)
- [Composer](#)
- [Discussion Server](#)
- [Analytics](#)
- [Activity Graph](#)
- [Personalization Server](#)
- [Portals](#)
- [Composite Applications](#)

Figure 1–1 Oracle WebCenter Portal Architecture



1.2.1 WebCenter Portal: Framework

Injects portal capabilities into ADF, including:

- Run-time application customization (you can make in-place changes to WebCenter Portal applications using Composer without re-deploying the application)
- Support for JSR-168 and JSR-286 standards-based WSRP portlets, and PDK-Java portlets
- Content integration through JCR (JSR170), to content repositories such as Oracle WebCenter Content Server, Oracle Portal, and file systems
- Oracle JSF Portlet Bridge, which lets you expose JSF pages and Oracle ADF task flows as standards-based portlets

1.2.2 Application Development Framework

The Oracle Application Development 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 Composer

Composer provides:

- Ability to perform run-time application and user customization in-place in your browser

- A rich, intuitive user experience where you can:
 - Browse and add resources, such as task flows and portlets, to pages
 - Re-arrange page layout
 - Set page and component properties
 - Contextually wire components

1.2.4 WebCenter Portal: Spaces

A WebCenter Portal application built using JSF, Oracle ADF, WebCenter Portal: Framework, WebCenter Portal: Services, and Composer. The Spaces application provides:

- a browser-based platform for creating enterprise portals, multiple sites and communities
- a Home space for each user, providing a private work area for storing personal content, keeping notes, viewing and responding to business process assignments, emailing, and so on
- threaded discussions, blogs, wikis, worklists, announcements, RSS, recent activities, search, and more.

1.2.5 WebCenter Portal: Services

Table 1–1 lists WebCenter Portal services available in WebCenter Portal applications.

Table 1–1 WebCenter Portal Services

Services A Through N	Services P Through W
Analytics	Page
Announcements	People Connections
Discussions	Personalization
Documents (includes Wikis and Blogs)	Polls
Events ²	RSS ¹
Instant Messaging and Presence (IMP)	Recent Activities
Links	Activity Graph
Lists ²	Search
Mail	Tags
Notes ²	Worklist

¹ RSS news feeds are available from Spaces only. The RSS Viewer task flow is available in Spaces and other WebCenter Portal applications.

² Spaces only.

WebCenter Portal services provide:

- Seamless integration with enterprise-level services
- Thin adapter layer to abstract back-end services. For example:
 - Content adapters: Oracle WebCenter Content Server, and Oracle Portal.

- Presence adapters: Microsoft Live Communications Server, Microsoft Office Communications Server, and Microsoft Lync
- Back-end systems represented by a unified connection architecture
- User interface to services presented through rich task flow components

1.2.6 Discussion Server

A discussion server is provided with WebCenter Portal so you can integrate discussion forums and announcements into your applications.

1.2.7 Analytics

WebCenter Portal's analytics capability enables users to view various user activity reports, for example:

- Login data
- Page views
- Portlet views
- Document views
- Search metrics
- Page response data
- Space usage

1.2.8 Activity Graph

The Activity Graph service in WebCenter Portal enables users to analyze various statistics collected by WebCenter Portal analytics. Various similarity scores for objects and users are collected, and used to give recommendations. The scores are stored in an Activity Graph database.

1.2.9 Personalization Server

WebCenter Portal's Personalization server enables you to deliver application content to targeted users based on selected criteria.

1.2.10 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 Portal*.

1.2.11 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 and Oracle Business Process Management Suite*.

1.3 Oracle WebCenter Portal Topology

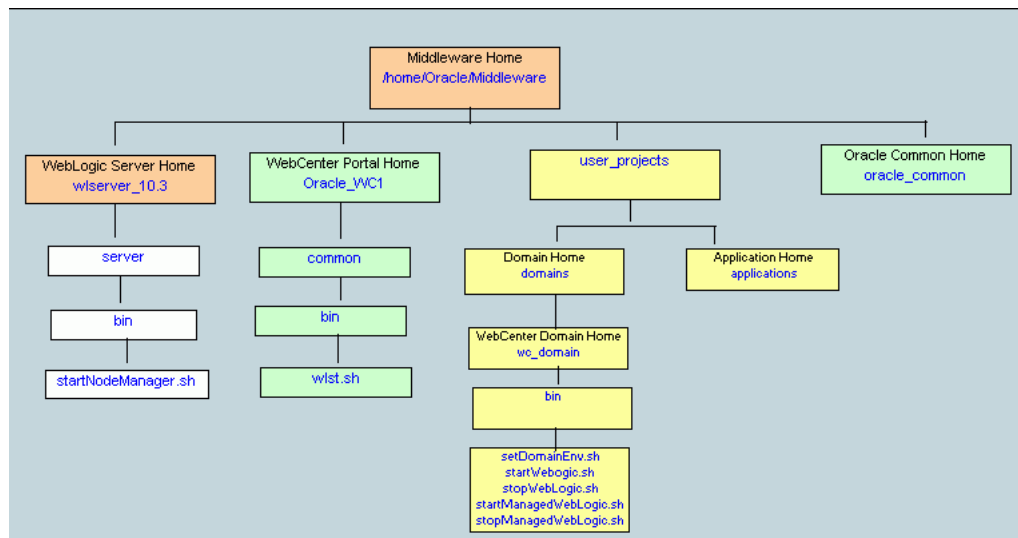
This section describes Oracle WebCenter Portal topology and configuration in the following sections:

- Section 1.3.1, "WebCenter Portal Topology Out-of-the-Box"
- Section 1.3.2, "WebCenter Portal Managed Servers"
- Section 1.3.3, "WebCenter Portal Startup Order"
- Section 1.3.4, "WebCenter Portal Dependencies"
- Section 1.3.5, "WebCenter Portal Configuration Considerations"
- Section 1.3.6, "WebCenter Portal State and Configuration Persistence"
- Section 1.3.7, "WebCenter Portal Log File Locations"

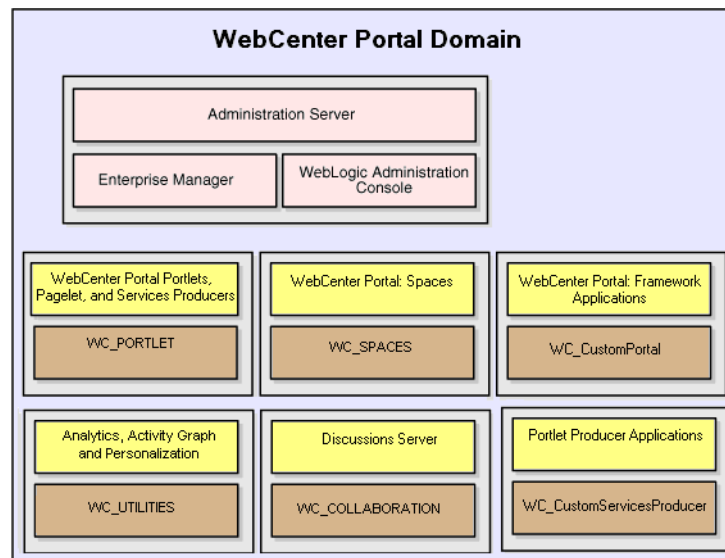
1.3.1 WebCenter Portal Topology Out-of-the-Box

Oracle WebCenter Portal installation creates a **WebCenter Portal Oracle Home** under the Oracle Middleware Home directory and an **Oracle Common Home** directory, which contains WebCenter Portal binaries and supporting files (Figure 1–2).

Figure 1–2 Directory Structure of an Oracle WebCenter Portal Installation



The installation also creates a WebCenter Portal domain (`base_domain`), containing the administration server and several managed servers to host various WebCenter Portal components. In Figure 1–3, applications are shown in yellow, while the managed servers they run on are shown in brown.

Figure 1–3 Oracle WebCenter Portal Topology Out-of-the-Box

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

- WC_Spaces - Hosts the Spaces application
- WC_Portlet - Hosts out-of-the-box portlets, the Pagelet Producer, and WebCenter Services Producer
- WC_Collaboration - Hosts the discussions server and any additional WebCenter Portal services that you choose to integrate
- WC_Uilities - Hosts Activity Graph, Analytics, and Personalization services

An optional fifth managed server (an applications server) can be used to run applications built by developers using WebCenter Portal: Framework—such applications are referred to as *Framework 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 the Spaces application. For more information about managed servers, see "Understanding Oracle Fusion Middleware Concepts" in the *Oracle Fusion Middleware Administrator's Guide*.

1.3.2 WebCenter Portal Managed Servers

During Oracle WebCenter Portal installation, the managed servers are provisioned with system libraries and Oracle ADF libraries. [Table 1–2](#) lists the managed servers and the applications that run on them.

Table 1–2 Oracle WebCenter Portal Managed Servers and Applications

Managed Server	Installed Applications	Application Name
WC_Spaces	Spaces	webcenter
	Spaces Online Help	webcenter-help

Table 1–2 (Cont.) Oracle WebCenter Portal Managed Servers and Applications

Managed Server	Installed Applications	Application Name
WC_Portlet	OmniPortlet and Web Clipping	portalTools
	WSRP Tools	wsrp-tools
	Pagelet Producer	pagelet-producer
	WebCenter Services Producer	services-producer
WC_Collaboration	Discussions Server	owc_discussions
WC_Utilities	Analytics Collector	analytics-collector
	Activity Graph Engines	activitygraph-engines
	Personalization Services	wcps-services

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

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

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 1.3.4, "WebCenter Portal Dependencies."](#)

1.3.4 WebCenter Portal Dependencies

WebCenter Portal applications use several external servers and services ([Table 1–3](#)). The Configuration column lists the type of information provided to WebCenter Portal to configure or initialize the connection. The Access column lists the protocol used in run-time access of the service.

Table 1–3 Dependent Resources - Access Types

External Server/ Service	Configuration	Access
Analytics	UDP access to the Analytics Collector	UDP
Activity Graph	HTTP access to activity graph administration	HTTP
Discussions server	HTTP access to discussions server administration	SOAP/HTTP
Oracle WebCenter Content Server (Documents)	Socket connection to the Administration Server. HTTP access is required only if the Oracle WebCenter Content Server must be accessed outside WebCenter.	JCR 1.0 over socket or HTTP

Table 1–3 (Cont.) Dependent Resources - Access Types

External Server/Service	Configuration	Access
Instant Messaging and Presence server	HTTP access to instant messaging and presence server administration	SOAP/HTTP
Mail server	IMAP/SMTP server	IMAP/SMTP
Personal Events server	HTTP access to calendar services	SOAP/HTTP
Personalization server	JDBC access to the personalization server	JDBC REST
Portlets	HTTP location of provider WSDLs	SOAP/HTTP
Search server	HTTP access to search server	HTTP
Worklist	HTTP access to BPEL server	SOAP/HTTP
MDS and Schemas	JDBC	JDBC

Server/service unavailability does not prevent WebCenter Portal applications from starting up, although errors may display while the application is running. The only exception is the Oracle Metadata Repository (MDS), as WebCenter Portal applications do not work without it.

Spaces partially works without the WebCenter Portal repository but only if it is a different physical database from the MDS repository. The WebCenter Portal repository stores information for several services, including Events, Links, Lists, People Connections, Polls, and Tags, and these services do not work if the WebCenter Portal repository is not available.

1.3.5 WebCenter Portal Configuration Considerations

The main configuration files for WebCenter Portal applications are listed and described in [Table 1–4](#). Both these files are supplied within the WebCenter Portal application deployment .EAR file.

Table 1–4 WebCenter Portal Configuration Files

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

WebCenter Portal 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 Portal applications and portlet producers as application customizations. MDS uses the original deployed versions of `adf-config.xml` and `connections.xml` as base documents and stores all subsequent application customizations separately into MDS using a single customization layer.

When a WebCenter Portal application starts up, application customizations stored in MDS are applied to the appropriate base documents and the WebCenter Portal

application uses the merged documents (base documents with customizations) as the final set of configuration properties.

For WebCenter Portal 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 `adf-config.xml` and `connections.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 Portal Configuration"](#).

To find out more about WebCenter Portal application configuration tools available, see [Section 1.13, "Oracle WebCenter Portal Administration Tools."](#)

Note: Oracle does not recommend that you edit `adf-config.xml` or `connections.xml` by hand as this can lead to misconfiguration.

While WebCenter Portal applications store post deployment configuration information in MDS, configuration information for portlet producers and the discussion server is stored in the file system or the database (see [Table 1–5](#)).

Table 1–5 WebCenter Portal Configuration Location

Application	Configuration Stored in MDS	Configuration Stored in File System	Configuration Stored in Database
Spaces application	Yes	No	No
Framework applications	Yes	No	No
Portlet producers	No	Yes	No
Discussions server	No	Yes	Yes

Discussions Server

WebCenter Portal's discussions server stores configuration information in its database. Additionally, it stores startup configuration information in `$DOMAIN_HOME/config/fmwconfig/servers/WC_COLLABORATION/owc_discussions`. This directory contains `jive_startup.xml`, `jive.license` files, and a `logs` directory containing log files for the discussions server instance.

1.3.6 WebCenter Portal State and Configuration Persistence

WebCenter Portal 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.

Application customizations within a portlet or service environment are persisted by that service. Out-of-the-box, Oracle portlets, any custom portlets you build, and the discussions server, all have their own database persistence mechanisms.

Analytics

WebCenter Portal's analytics capability is stateless. Requests received by analytics collectors are executed immediately. Any in-transit state, such as a request initiated by

a WebCenter Portal application or a request processed by the analytics collector, is not guaranteed.

Activity Graph

WebCenter Portal's Activity Graph consists of two components:

- **Activity Graph service** - does not maintain any in-memory state. The Activity Graph task flows query the Activity Graph database and display results as a list of recommendations. State is updated by the following:
 - Task flow configuration parameters
 - Personalization settings
 - "Not-interested" feature

The first two are built on the standard Oracle Composer/Oracle ADF/MDS framework, which manages the state. The last is a feature where the user can indicate that they are not interested in a particular recommendation. This input is persisted synchronously in the database.

- **Activity Graph Engine** - runs a batch data analysis process that updates tables in the database transactionally. Although the engine does not support clustering or failover, it can recover from failure.

Administrators use the Activity Graph Scheduler to set up and monitor the nightly schedule. The results of the analysis (the recommendations) are presented through the Activity Graph task flows.

The Activity Graph Engine is a singleton application that has a background thread that wakes up periodically to check if it is time to run the nightly job, which can last several hours. The schedule is persisted in the database. If the managed server fails, the job continues when the managed server next starts up.

Personalization Server

WebCenter Portal's Personalization Server is a stateless RESTful application. All state is managed in the client requests.

1.3.7 WebCenter Portal Log File Locations

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

```
<base_domain>/servers/<WC_Server>/logs/<WC_Server>-diagnostic.log
```

For example, diagnostics for the Spaces application are logged to:

```
/base_domain/servers/WC_Spaces/logs/WC_Spaces-diagnostic.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 38.3, "Viewing and Configuring Log Information."](#)

1.4 Spaces Application

Spaces is a Web-based application that offers the very latest technology for social networking, communication, collaboration, and personal productivity. Through a robust set of services and applications, *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.

Automatic Configuration for Services

Some services are automatically configured for the *Spaces* application during the installation process. For details, see *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Portal*.

Default connection names are listed in [Table 1–6](#).

Table 1–6 Connections Automatically Configured for the Spaces Application

WebCenter Portal Service / Component	Default Connection Name
Discussions and Announcements services	WebCenterSpaces-Discussions
Documents service	WebCenterSpaces-ucm
Pagelet producer	WebCenterSpaces-PageletProducer
Personalization service	Conductor-WCPSSpaces and Properties-WCPSSpaces
Preconfigured portlet producers	wc-OmniPortlet
	wc-WebClipping
	wc-WSRPTools
Worklist service	WebCenterSpaces-Worklist
Spaces workflows	

Configuring the Spaces Application PostInstallation

To help you get started, see:

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

For information about administering *Spaces*, see "Accessing *Spaces* Administration Pages" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

1.5 Framework Applications

You can develop your own portal applications using JDeveloper and WebCenter Portal: Framework, and deploy them to a custom WebLogic Managed Server. Portal applications built using WebCenter Portal: Framework are referred to as *Framework applications*.

For information about developing your own portal applications, see the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

To help you get started, see:

- [Chapter 4, "Getting Framework Applications Up and Running"](#)
- [Chapter 5, "Maintaining Framework Applications"](#)
- [Chapter 7, "Deploying WebCenter Portal: Framework Applications"](#)

1.6 Planning WebCenter Portal Installations

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

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

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

1.7 Understanding the WebCenter Portal 11g Installation

The out-of-the-box WebCenter Portal topology is briefly described in [Section 1.3, "Oracle WebCenter Portal Topology"](#). Specific areas of the WebCenter Portal topology are described in the corresponding chapters, for example, security-related aspects of the WebCenter Portal topology are described in [Chapter 28, "Managing WebCenter Portal Application Security."](#)

For more information about Oracle WebCenter Portal installation and postinstallation administration tasks, see *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Portal*.

For postinstallation enterprise configuration, see the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle WebCenter Portal*.

For postinstallation high availability configuration, see the *Oracle Fusion Middleware High Availability Guide*.

For postinstallation security configuration, see [Chapter 28.2.5, "Post-deployment Security Configuration Tasks."](#)

1.8 Understanding Administrative Operations, Roles, and Tools

Oracle WebCenter Portal provides several different tools with which to deploy, configure, start and stop, and maintain WebCenter Portal applications. All these tools are described in [Section 1.13, "Oracle WebCenter Portal Administration Tools."](#)

Your ability to perform WebCenter Portal administration tasks depends on which Oracle WebLogic Server role you are assigned—Admin, Operator, or Monitor. [Table 1-7](#) 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 1-7 WebCenter Portal Operations and Oracle WebLogic Server Roles

Operation	Admin Role	Operator Role	Monitor Role
All WebCenter Portal applications			
Start and stop	Yes	Yes	No
View performance metrics	Yes	Yes	Yes

Table 1–7 (Cont.) WebCenter Portal Operations and Oracle WebLogic Server Roles

Operation	Admin Role	Operator Role	Monitor Role
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
Spaces application only			
Export Spaces	Yes	No	No
Import Spaces	Yes	No	No

Table 1–8 summarizes which tools you can use to perform various administrative operations relating to WebCenter Portal applications.

Table 1–8 WebCenter Portal Operations and Administration Tools

Operation	Fusion Middleware Control	WLST Commands	WebLogic Server Admin Console	Spaces Application Admin
All WebCenter Portal applications				
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
Manage portlet producers	Yes	Yes	No	Yes
Manage external applications	Yes	Yes	No	Yes
Deploy applications	Yes	Yes	Yes	No
Configure security	Yes	Yes	Yes	No
Spaces application only				
Configure workflows	Yes	Yes	No	No
Export Spaces application	Yes	Yes	No	No
Import Spaces application	Yes	Yes	No	No

Table 1–8 (Cont.) WebCenter Portal Operations and Administration Tools

Operation	Fusion Middleware Control	WLST Commands	WebLogic Server Admin Console	Spaces Application Admin
Customize Spaces application	No	No	No	Yes
Manage application users and roles	No	No	No	Yes
Manage pages	No	No	No	Yes
Manage spaces	No	No	No	Yes
Export individual spaces	No	No	No	Yes
Import individual spaces	No	No	No	Yes

1.9 Performance Monitoring and Diagnostics

Performance monitoring helps administrators identify issues and performance bottlenecks in their environment. [Chapter 38, "Monitoring Oracle WebCenter Portal Performance"](#) describes the range of performance metrics available for WebCenter Portal 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 Portal diagnostic log files.

1.10 Understanding Security

The recommended security model for Oracle WebCenter Portal is based on Oracle ADF Security, which implements the Java Authentication and Authorization Service (JAAS) model. The following chapters describe security configuration for WebCenter Portal applications:

- [Chapter 28, "Managing WebCenter Portal Application Security."](#)
- [Chapter 29, "Configuring the Identity Store"](#)
- [Chapter 30, "Configuring the Policy and Credential Store"](#)
- [Chapter 31, "Configuring Single Sign-on"](#)
- [Chapter 32, "Configuring Framework Applications for Single Sign-on"](#)
- [Chapter 33, "Configuring SSL"](#)
- [Chapter 34, "Configuring WS-Security"](#)
- [Chapter 35, "Configuring Security for Portlet Producers"](#)

1.11 WebCenter Portal Application Deployment

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

[Section 24.8, "Deploying Portlet Producer Applications"](#) provides instructions for deploying WSRP and PDK-Java portlet producer applications.

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

1.12 Data Migration, Backup, and Recovery

Oracle WebCenter Portal 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 Portal provides a set of utilities that enable you to back up this data, and move the data between WebCenter Portal application staging and production environments.

[Chapter 39, "Managing Export, Import, Backup, and Recovery of WebCenter Portal"](#) describes the backup, import, and export capabilities and tools available for these tasks.

1.13 Oracle WebCenter Portal Administration Tools

Oracle offers the following tools for managing WebCenter Portal:

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

These administration tools apply to all WebCenter Portal applications, including Spaces, and administrators should use these tools, rather than edit configuration files, to perform administrative tasks. For help to decide which tool is best for you, see [Appendix A.3, "Configuration Tools"](#).

In addition to system administrative tools, individual applications also offer some runtime administration pages:

- [Spaces Administration Pages](#)
- [WebCenter Portal Administration Console](#)

1.13.1 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 Portal. From Fusion Middleware Control Console, you can monitor and administer a *farm* (such as one containing Oracle WebCenter Portal and WebCenter Portal 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 Portal 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 Portal and can be used to:

- Deploy, undeploy, and re-deploy WebCenter Portal 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

1.13.1.1 Displaying Fusion Middleware Control Console

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

1.13.2 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

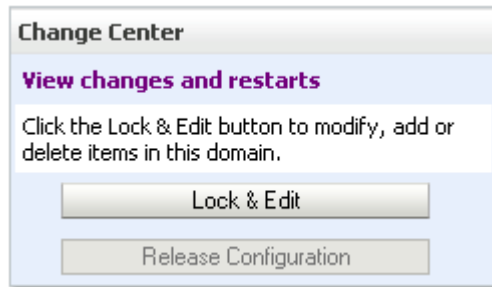
For more information about the Oracle WebLogic Server Administration Console, see "Displaying the Oracle WebLogic Server Administration Console" in the *Oracle Fusion Middleware Administrator's Guide*.

Locking Domain Configuration

You must lock configuration settings for a domain before making any configuration changes. Navigate to the Administration Console's Change Center ([Figure 1-4](#)), and click **Lock & Edit**.

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

Figure 1–4 Change Center in Oracle WebLogic Server Administration Console



1.13.3 Oracle WebLogic Scripting Tool (WLST)

Oracle provides the WebLogic Scripting Tool (WLST) to manage Oracle Fusion Middleware components, such as Oracle WebCenter Portal, 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 provides WLST commands for managing WebCenter Portal application connections (to content repositories, portlet producers, external applications, and other back-end services), and application migration. All WebCenter Portal WLST commands are described in "WebCenter Portal Custom WLST Commands" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

1.13.3.1 Running Oracle WebLogic Scripting Tool (WLST) Commands

You *must* run all WebCenter Portal WLST commands from your **WebCenter Portal Oracle home directory** (`WC_ORACLE_HOME`).

Note: If you attempt to run WebCenter Portal WLST commands from the wrong directory you will see a `NameError`. To avoid this error, always run WebCenter Portal WLST commands from WebCenter Portal Oracle home (`WC_ORACLE_HOME/common/bin`) as directed below.

See also, [Section A.6, "Troubleshooting WLST Command Issues"](#).

To run WLST from the command line:

1. Navigate to your **WebCenter Portal Oracle home** directory and invoke the WLST script:

```
(UNIX)    WC_ORACLE_HOME/common/bin/wlst.sh
```

```
(Windows) WC_ORACLE_HOME\common\bin\wlst.cmd
```

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


```
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(username='weblogic', password='mypassword',
url='myhost.example.com:7001')
```

If preferred, you can connect to the Administration Server in interactive mode without parameters:

```
wls:/offline> connect()
Please enter your username :weblogic
Please enter your password :
Please enter your server URL [t3://localhost:7001]:t3://myhost.example.com:7001
Connecting to t3://myhost.example.com:7001 with userid weblogic ...
Successfully connected to Admin Server 'AdminServer' that belongs to domain
'wc_domain'.
```

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

Note: If SSL is enabled, you must edit the `wlst.sh` or `wlst.cmd` 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
```

3. Once connected to the Administration Server you can run WebCenter Portal WLST commands, and any other generic WLST command.

Hints and Tips Running for WebCenter Portal WLST Commands

- **To list WebCenter Portal WLST commands**, type: `help('webcenter')` at the WLST command prompt.

If the message `No help for webcenter found...` displays, you are probably running the WLST script from the wrong directory, for example, you might be running `wlst.sh` or `wlst.cmd` from the `oracle_common` directory instead of `WC_ORACLE_HOME/common/bin`.

- **For help on a particular command**, type: `help('WLST_command_name')` at the WLST command prompt.
- **Include argument names when running commands** and especially when writing WLST scripts. For example, it is good practice to enter:

```
createExtAppConnection (appName='webcenter', name='myXApp' ...
```

rather than:

```
createExtAppConnection ('webcenter', 'myXApp' ...
```

Either syntax is valid but when you include the argument names, errors and misconfiguration is less likely. Also, if arguments are added in the future, the command does not fail or configure the wrong property.

- **Online documentation for WebCenter Portal WLST commands** is available from "WebCenter Portal Custom WLST Commands" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

1.13.4 System MBean Browser

Fusion Middleware Control provides a set of MBean browsers that allow you to browse the MBeans for an Oracle WebLogic Server or for a selected application.

Note: While you can monitor and configure WebCenter Portal application MBeans from the System MBean browser, it is not the preferred tool for configuration. Oracle recommends that you configure WebCenter Portal applications using WLST commands or through the **WebCenter Portal Settings** menu options in Fusion Middleware Control (available from the application's home page).

To access application MBeans for WebCenter Portal applications:

1. Log in to Fusion Middleware Control and navigate to the home page for Spaces or your Framework application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **System MBean Browser**.
 - For Framework applications - From the **Application Deployment** menu, choose **System MBean Browser**.
3. Expand **Application Defined MBeans**.
4. Navigate to the MBean you want to view or configure.

For example, for a Framework applications, you might want to navigate to MBeans for `adf-config.xml` and `connections.xml` as follows ([Figure 1-5](#)):

- `adf-config` - Click **oracle.adf.share.config >Server: name >Application: name >ADFConfig >ADFConfig >ADFConfig**
 - `connections` - Click **oracle.adf.share.connections >Server: name >Application: name >ADFConnections >ADFConnections**
5. To view an MBean's attributes, select the **Attributes** tab. Some attributes allow you to change their values. To do so, enter the value in the **Value** column.

Figure 1–5 Systems MBean Browser

The screenshot shows the System MBean Browser interface. On the left, a tree view displays the MBean hierarchy. The 'ADFConfig' MBean is selected, and its parent 'ADFConnections' is also highlighted. On the right, the 'Application Defined MBeans: BPEL:WebCenter-Worklist' section is expanded, showing a table of attributes. The 'PolicyURI' attribute is highlighted with a red box, and its value 'oracle/wss10_sa' is also highlighted. A red arrow points from the 'PolicyURI' attribute name to the label 'MBean Name' below. Another red arrow points from the 'PolicyURI' value to the label 'MBean Value' below. The 'URL' attribute is also highlighted with a red box, and its value 'http://owcsvr02.' is highlighted. A red arrow points from the 'URL' attribute name to the label 'MBean Name' below. Another red arrow points from the 'URL' value to the label 'MBean Value' below.

Name	Description	Access	Value
1 ConfigMBean	If true, it indicates that this MBean is a Config MBean.	R	false
2 ConnectionClassName	Attribute exposed for management	R	oracle.adf.mbean
3 ConnectionName	Attribute exposed for management	R	WebCenter-Workl
4 ConnectionType	Attribute exposed for management	R	BPEL
5 eventProvider	If true, it indicates that this MBean is an event provider as defined by JSR-77.	R	true
6 eventTypes	All the event's types emitted by this MBean.	R	jmx.attribute.char
7 LinkURL	The link URL of the BPEL connection.	RW	
8 objectName	The MBean's unique JMX name	R	oracle.adf.share.c
9 PolicyURI	The SAML Token Policy URI of the BPEL connection.	RW	oracle/wss10_sa
10 ReadOnly	If true, it indicates that this MBean is a read only MBean.	R	false
11 RecipientKeyAlias	The recipient key alias of the BPEL connection.	RW	
12 RestartNeeded	Indicates whether a restart is needed.	R	false
13 stateManageable	If true, it indicates that this MBean provides State Management capabilities as defined by JSR-77.	R	false
14 statisticsProvider	If true, it indicates that this MBean is a statistic provider as defined by JSR-77.	R	false
15 SystemMBean	If true, it indicates that this MBean is a System MBean.	R	false
16 URL	The service URL of the BPEL connection.	RW	http://owcsvr02.

6. Click **Apply** to update attribute values.
7. Navigate to the parent MBean (for example, **ADFConfig** or **ADFConnections**), select the **Operations** tab, and click **save** to save the changes.
8. Restart the managed server on which the WebCenter Portal application is deployed. For more information, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

1.13.5 Spaces Administration Pages

The Spaces application provides several administration pages of its own. The administration pages appear only to users who have logged in to the application using an administrator user name and password.

Spaces administration pages allow you to:

- Customize the Spaces application
- Manage users and roles
- Manage services settings for the Spaces application
- Manage portlet producers and external applications
- Manage individual spaces and space templates
- Create and manage business role pages
- Manage personal pages
- Export and import individual spaces and space templates

For more details, see "Accessing Spaces Administration Pages" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

1.13.6 WebCenter Portal Administration Console

Portal applications built using WebCenter Portal: Framework can also include administration pages that enable administrators to perform common administrative duties at runtime. For more information, see [Chapter 36, "Using WebCenter Portal Administration Console"](#).

Part II

Getting Started With Oracle WebCenter Portal Administration

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

Part II contains the following chapters:

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

Getting the Spaces Application Up and Running

Getting WebCenter Portal's Spaces application up and running and ready for use requires input from both the *Fusion Middleware administrator* and the *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 Spaces up and running. Some roadmaps are provided to guide you through this process.

This chapter includes the following sections:

- [Section 2.1, "Role of the Fusion Middleware Administrator"](#)
- [Section 2.2, "Role of the Spaces Administrator"](#)
- [Section 2.3, "Installing WebCenter Portal: Spaces"](#)
- [Section 2.4, "Setting Up Spaces for the First Time \(Roadmap\)"](#)
- [Section 2.5, "Customizing Spaces for the First Time \(Roadmap\)"](#)

Audience

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

Note: Administrators working with portal applications developed using WebCenter Portal: Framework, should refer to [Chapter 4, "Getting Framework 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, and all installation, configuration, and audit tasks. This administrator is also responsible for setting up and configuring the Spaces application immediately after installation, and performing on-going administrative tasks for Spaces and other Oracle WebCenter Portal components. Throughout this document, this administrator is referred to 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 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 Application 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 1–7, "WebCenter Portal Operations and Oracle WebLogic Server Roles"](#) in [Section 1.8, "Understanding Administrative Operations, Roles, and Tools"](#).

- **Spaces Administration** - Assign one more users the `Administrator` role through Spaces administration pages. For details, "Giving a User Administrative Privileges" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

To find out what other tasks a Fusion Middleware administrator must do to get Spaces up and running, follow the steps listed under "[Roadmap - Setting Up the Spaces Application 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 Spaces \(Roadmap\)"](#).

2.2 Role of the Spaces Administrator

Spaces administrators have the highest application privileges within the Spaces application itself. This administrator can view and customize every aspect of the Spaces application, manage users and roles, and delegate responsibilities to others.

Out-of-the-box, the default Fusion Middleware administrator (`weblogic`) is the only user assigned to the `Spaces Administrator` role. The password is the one provided during installation. Use this administrator account to log in to Spaces, and assign additional users the `Administrator` role. For details, see "Giving a User Administrative Privileges" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

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

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

2.3 Installing WebCenter Portal: Spaces

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

2.4 Setting Up Spaces for the First Time (Roadmap)

The flow chart depicted in Figure 2-1 and Table 2-1 in this section provide an overview of the tasks required to get the Spaces application up and running.

Figure 2-1 Setting Up the Spaces Application for the First Time

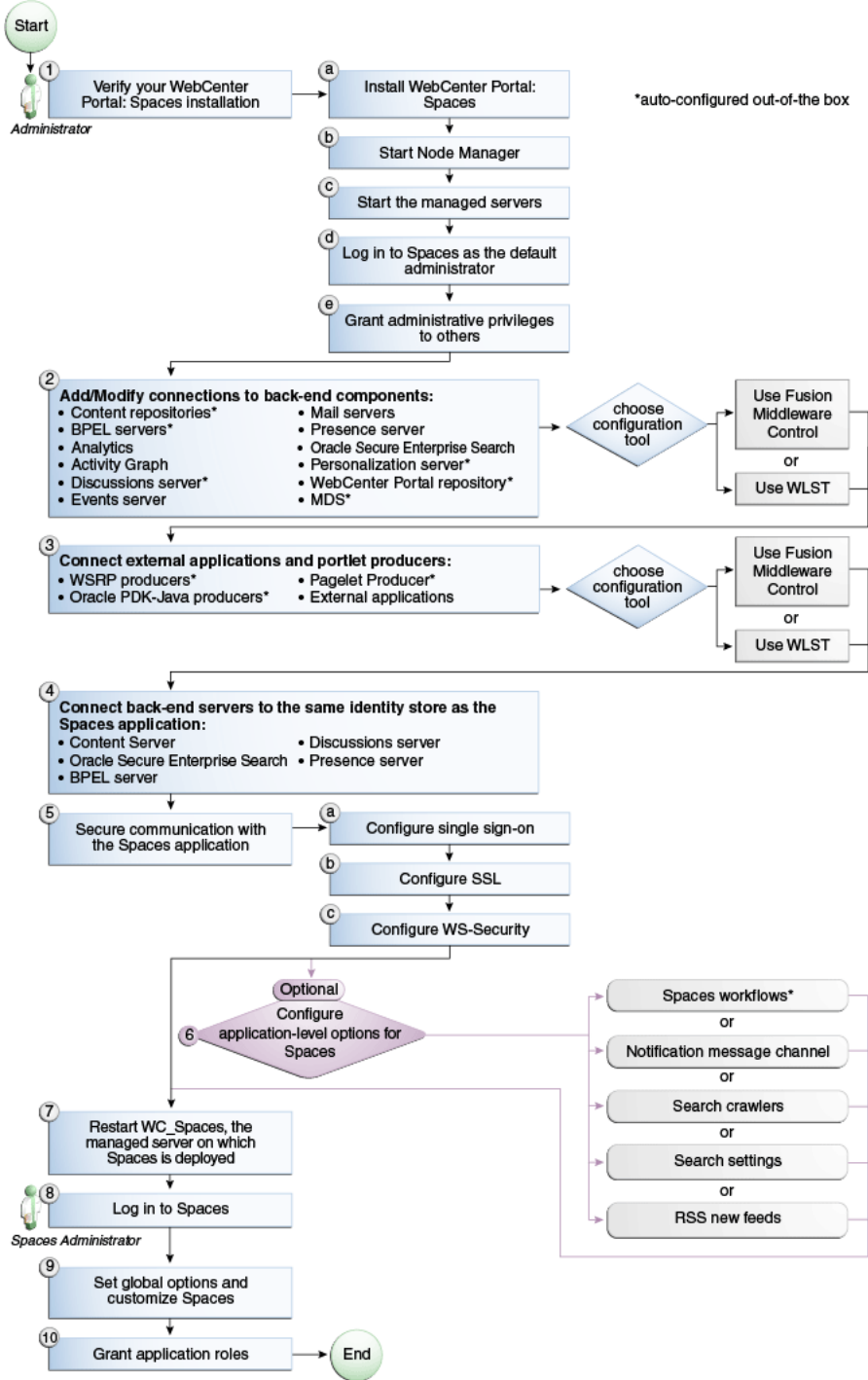


Table 2–1 Roadmap - Setting Up the Spaces Application for the First Time

Actor	Task	Sub-task	Notes
Administrator	1. Verify your Spaces installation	<p>1.a Install WebCenter Portal: Spaces</p> <p>1.b Start Node Manager</p> <p>1.c Start the managed servers</p> <p>1.d Log in to the Spaces application as the default administrator</p> <p>1.e Grant administrative privileges to others</p>	
Administrator	<p>2. Add/modify connections to back-end components using either of the following tools:</p> <ul style="list-style-type: none"> ■ Fusion Middleware Control ■ WLST 		<p>Back-end components may include:</p> <ul style="list-style-type: none"> ■ Content repositories¹ ■ BPEL servers¹ ■ Analytics Collector ■ Activity Graph Engines ■ Discussions server¹ ■ Events server ■ Mail servers ■ Presence server ■ Oracle Secure Enterprise Search ■ Personalization server¹ ■ WebCenter Portal repository¹ ■ MDS¹
Administrator	<p>3. Connect external applications and portlet producers using either of the following tools:</p> <ul style="list-style-type: none"> ■ Fusion Middleware Control ■ WLST 		<p>Portlet producers may include:</p> <ul style="list-style-type: none"> ■ WSRP producers¹ ■ Oracle PDK-Java producers¹ ■ Pagelet producer¹

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

Actor	Task	Sub-task	Notes
Administrator	4. Connect back-end servers to the same identity store as the Spaces application		Back-end servers may include: <ul style="list-style-type: none"> ■ Oracle WebCenter Content Server ■ Oracle Secure Enterprise Search ■ BPEL server ■ Discussions server ■ Presence server
Administrator	5. Secure communication with the Spaces application	5.a Configure single sign-on 5.b Configure SSL 5.c Configure WS-Security	
Administrator	6. (Optional) Configure Spaces options: <ul style="list-style-type: none"> ■ Spaces workflows¹ ■ Notification message channel ■ Search crawlers ■ Search settings ■ RSS news feeds 		
Administrator	7. Restart WC_Spaces, the managed server on which the Spaces application is deployed		
Spaces Administrator	8. Log in to Spaces		
Spaces Administrator	9. Set global options and customize Spaces		
Spaces Administrator	10. Grant application roles		

¹ Auto-configured out-of-the-box

2.5 Customizing Spaces for the First Time (Roadmap)

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

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

Task	Documentation	Actor
1. Log in to Spaces	<p>Login to Spaces with administrative privileges and access the administration pages:</p> <ul style="list-style-type: none"> ■ Accessing Spaces Administration Pages <p>Tips:</p> <p>Spaces URL is <code>http://<host>:<port>/webcenter</code></p> <p>Spaces Administration URL is <code>http://<host>:<port>/webcenter/spaces/admin</code></p>	Spaces Admin
2. Customize Spaces	<p>Customize Spaces to suit your audience. Choose a name and logo for your application, apply a corporate brand, set language options, and more. For details, see:</p> <ul style="list-style-type: none"> ■ Performing Actions on Spaces Administration Pages ■ Configuring Global Defaults ■ Configuring Services, Portlet Producers, and External Applications ■ Preparing Your Initial Portal Pages ■ Managing Portal Resources 	Spaces Admin
3. Determine self-registration policy	<p>Establish your policy regarding new user registration. Allow users outside of the Spaces community to self-register on an invitation-only basis or extend self-registration to the public:</p> <ul style="list-style-type: none"> ■ Enabling Self-Registration By Invitation-Only ■ Enabling Anyone to Self-Register 	Spaces Admin
4. Plan the public user experience	<p>First impressions are extremely important. Determine the content displayed on your Welcome page and the appearance of Spaces before users login:</p> <ul style="list-style-type: none"> ■ Customizing the Welcome Page ■ Customizing the Login Page ■ Customizing the Self-Registration Page ■ Choosing the Default Display Language ■ Granting Permissions to the Public-User 	Spaces Admin
5. Create roles and delegate responsibilities to other users	<p>Create roles to characterize groups of users and determine what they can see and do in the Spaces application. Manage and assign roles for any user in the identity store:</p> <ul style="list-style-type: none"> ■ Introduction to Security in Spaces ■ Assigning Users (and Groups) to Roles ■ Defining Application Roles ■ Giving a User Administrative Privileges ■ Modifying Application Role Permissions 	Spaces Admin

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

Task	Documentation	Actor
6. Customize the Home space	<p>Design the default Home space for Spaces users. Give them instant access to important information and applications relevant to their roles:</p> <ul style="list-style-type: none"> ■ Setting Page Creation Defaults for Business Role Pages ■ Creating a Business Role Page <p>Encourage or enforce a consistent look and feel through default page schemes and default page templates:</p> <ul style="list-style-type: none"> ■ Choosing a Default Look and Feel for New Pages 	Spaces Admin
7. Set up discussion forums and announcements	<p>Configure default options for discussion forums and announcements:</p> <ul style="list-style-type: none"> ■ Configuring Discussion Forum Options for Spaces 	Spaces Admin
8. Set up people connection components	<p>Configure defaults for activity streams, personal profiles, connections, messages boards, and feedback:</p> <ul style="list-style-type: none"> ■ Configuring People Connection Defaults for Spaces 	Spaces Admin
9. Set up mail notifications	<p>Configure default options for everyone's mail:</p> <ul style="list-style-type: none"> ■ Configuring Send Mail Notifications for the Spaces application 	Spaces Admin
10. Provide ready-made spaces and space templates	<p>Users can create and manage their own spaces without centralized administration. Give them a head-start by creating templates for the types of workspaces and communities they are likely to build:</p> <ul style="list-style-type: none"> ■ Building a Space ■ Creating a Custom Space Template 	Spaces Admin

Maintaining the Spaces Application

Keeping the Spaces application up and running requires input from both the *Fusion Middleware administrator* and the *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:

- [Section 3.1, "Role of the Fusion Middleware Administrator"](#)
- [Section 3.2, "Role of the Spaces Administrator"](#)
- [Section 3.3, "System Administration for Spaces \(Roadmap\)"](#)
- [Section 3.4, "Application Administration for Spaces \(Roadmap\)"](#)

Audience

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

Note: Administrators maintaining portal applications built using the WebCenter Portal: Framework should refer to [Chapter 5, "Maintaining Framework Applications"](#).

3.1 Role of the Fusion Middleware Administrator

Oracle Fusion Middleware provides a single administrative role with complete administrative capabilities—the `Admin` role. The Fusion Middleware administrator can perform the complete range of security-sensitive administrative duties, and all installation, configuration, and audit tasks. This administrator is also responsible for setting up and configuring the Spaces application immediately after installation, and performing on-going administrative tasks for Spaces and other Oracle WebCenter Portal components. Throughout this document, this administrator is referred to 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 Spaces, follow the [Roadmap - Administering and Monitoring Spaces](#).

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

3.2 Role of the Spaces Administrator

Spaces administrators have the highest application privileges within the Spaces application itself. This administrator can view and customize every aspect of the Spaces application, manage users and roles, and delegate responsibilities to others.

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

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

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

3.3 System Administration for Spaces (Roadmap)

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

Table 3–1 Roadmap - Administering and Monitoring Spaces

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

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

Task	Documentation	Role
Monitor performance	Analyze the performance of the Spaces application and monitor its current status through Fusion Middleware Control Console: <ul style="list-style-type: none"> ■ Viewing Performance Information ■ Monitoring a Spaces Applications <p>Fusion Middleware administrators granted one of these roles can view performance metrics: Admin, Operator, Monitor. To find out more, see in "Understanding Administrative Operations, Roles, and Tools".</p> <p>Spaces administrators can monitor application performance and usage using WebCenter Portal's analytics feature:</p> <ul style="list-style-type: none"> ■ Understanding the Analytics Administration Page in WebCenter Spaces 	Fusion Middleware Admin Spaces Admin
Tune application properties	Reconfigure performance related parameters for the WebCenter Portal environment, Spaces application, and WebCenter Portal services: <ul style="list-style-type: none"> ■ Tuning Oracle WebCenter Portal Performance 	Fusion Middleware Admin
Stop and start Spaces	Fusion Middleware administrators may shut down the Spaces application for maintenance purposes and then restart the application: <ul style="list-style-type: none"> ■ Starting Spaces Using Fusion Middleware Control ■ Stopping Spaces Using Fusion Middleware Control 	Fusion Middleware Admin
Modify back-end services	Add, modify, and delete connections through Fusion Middleware Control Console. See: <ul style="list-style-type: none"> ■ Content Repositories ■ Managing Content Repositories ■ Mail Servers ■ Managing the Mail Service ■ BPEL Servers ■ Managing the Worklist Service ■ Collaboration Services ■ Managing the Announcements and Discussions Services ■ Managing the Instant Messaging and Presence Service ■ Calendar Services ■ Managing the Events Service ■ Secure Enterprise Search ■ Managing Oracle SES Search in WebCenter Portal ■ Analytics Services ■ Managing the Analytics Service ■ Activity Graph Services ■ Managing the Activity Graph Service ■ Personalization Services ■ Managing Personalization for WebCenter Portal ■ Events, Links, Lists, Notes, Tags, and People Connections ■ Setting Up Database Connections ■ Setting Up the MDS Repository 	Fusion Middleware Admin

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

Task	Documentation	Role
Modify external applications and portlet producers	Add, modify, and delete connections through Fusion Middleware Control Console. See: <ul style="list-style-type: none"> External Applications <ul style="list-style-type: none"> Managing External Applications Portlet Producers <ul style="list-style-type: none"> Registering WSRP Producers Registering Oracle PDK-Java Producers Registering the Pagelet Producer 	Fusion Middleware Admin
Configure SSL communication	Configure secure communication: <ul style="list-style-type: none"> Configuring SSL Configuring WS-Security Configuring Single Sign-on See also <i>Oracle Fusion Middleware Application Security Guide</i> .	Fusion Middleware Admin
Reassociate your identity, policy, and credential stores	Reassociate your identity or policy stores: <ul style="list-style-type: none"> Configuring the Identity Store Configuring the Policy and Credential Store See also <i>Oracle Fusion Middleware Application Security Guide</i> .	Fusion Middleware Admin
Reconfigure WebCenter Portal repository	Reconfigure the WebCenter Portal repository: <ul style="list-style-type: none"> Setting Up Database Connections 	Fusion Middleware Admin
Reconfigure MDS repository	Reconfigure the application's MDS repository: <ul style="list-style-type: none"> Setting Up the MDS Repository See also <i>Oracle Fusion Middleware Administrator's Guide</i> : <ul style="list-style-type: none"> Managing the MDS Repository Configuring an Application to Use a Different MDS Repository or Partition Moving Metadata from a Test System to a Production System 	Fusion Middleware Admin
Reconfigure Spaces workflows	Install Spaces workflows on a different BPEL server and reconfigure the connection: <ul style="list-style-type: none"> Installing Spaces Workflows Specifying the BPEL Server Hosting Spaces Workflows 	Fusion Middleware Admin
Export Spaces application	Use the export facility to move content to a remote instance or between stage and production environments: <ul style="list-style-type: none"> Exporting an Entire Spaces Application Exporting Individual Spaces Exporting Individual Space Templates 	Fusion Middleware Admin

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

Task	Documentation	Role
Import Spaces application	Use the import facility to restore Space from a backup or to move content to a remote instance or between stage and production environments: <ul style="list-style-type: none"> ■ Importing an Entire Spaces Application ■ Importing Individual Spaces ■ Importing Individual Space Templates 	Fusion Middleware Admin

3.4 Application Administration for Spaces (Roadmap)

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

If 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 Spaces Up and Running

Task	Documentation	Role
Modify application Settings	Modify application-wide settings as required: <ul style="list-style-type: none"> ■ Performing Actions on Spaces Administration Pages ■ Configuring Global Defaults ■ Configuring Services, Portlet Producers, and External Applications ■ Preparing Your Initial Portal Pages ■ Managing Portal Resources 	Spaces Admin
Manage Home apaces	Manage personal pages and business role pages. Push content to the Home space: <ul style="list-style-type: none"> ■ Working with Business Role Page ■ Working with Personal Pages ■ Working with System Pages 	Spaces Admin
Manage spaces	Take any space temporarily offline and close down any space that is inactive. Edit and delete any space: <ul style="list-style-type: none"> ■ Viewing Space Information ■ Changing the Status of a Space 	Spaces Admin
Manage space templates	Manage space templates. Review and delete any template: <ul style="list-style-type: none"> ■ Managing Space Templates 	Spaces Admin
Maintain users and roles	Maintain security. Modify user role permissions and assign new roles: <ul style="list-style-type: none"> ■ Modifying Application Role Permissions ■ Assigning a User to a Different Role 	Spaces Admin
Manage external applications	Maintain external applications. Add, modify, and delete entries: <ul style="list-style-type: none"> ■ Registering External Applications 	Spaces Admin AppConne ctionMana ger

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

Task	Documentation	Role
Manage portlet producers	Maintain portlet producers. Add, modify, and delete entries: <ul style="list-style-type: none">■ Registering Portlet Producers	Spaces Admin AppConnectionManager

Getting Framework Applications Up and Running

Framework applications are portal applications built using WebCenter Portal: Framework. The chapter outlines what Fusion Middleware administrators must do, after installation, to get Framework applications up and running. A roadmap is provided to help guide you through the process.

The chapter includes the following sections:

- [Section 4.1, "Installing Oracle WebCenter Portal and the Framework Libraries"](#)
- [Section 4.2, "Deploying Framework Applications for the First Time \(Roadmap\)"](#)

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

Audience

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

4.1 Installing Oracle WebCenter Portal and the Framework Libraries

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

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

Framework applications can be deployed to any WebLogic Server instance that is provisioned with WebCenter Portal's Framework shared library files. For details, see, [Section 7.1.4, "Creating a Managed Server"](#).

4.2 Deploying Framework Applications for the First Time (Roadmap)

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

Note: The Spaces application requires additional administration tasks that other Framework applications do not. To see a comprehensive list of these tasks, refer to [Chapter 2, "Getting the Spaces Application Up and Running"](#).

Table 4–1 Roadmap - Getting Framework Applications Up and Running for the First Time

Step	Documentation	Role
Step 1 - Verify your Oracle WebCenter Portal installation	<p>Verify your Oracle WebCenter Portal installation and settings. See:</p> <ul style="list-style-type: none"> ▪ Installing Oracle WebCenter Portal and the Framework Libraries ▪ Starting Node Manager 	Fusion Middleware Admin
Step 2 - Launch Fusion Middleware Control	<p>Launch the Fusion Middleware Control Console, a Web-based management tool for WebCenter Portal applications. See:</p> <ul style="list-style-type: none"> ▪ Displaying Fusion Middleware Control Console ▪ Navigating to the Home Page for Framework Applications <p>Learn about the command-line administration tool WLST. See "Oracle WebLogic Scripting Tool (WLST)".</p>	Fusion Middleware Admin
Step 3 - Deploy the Framework application	<p>Create a suitable container in which to deploy the Framework application archive:</p> <ul style="list-style-type: none"> ▪ Creating a Managed Server ▪ Creating and Registering the Metadata Service Repository ▪ Deploying the Application to a WebLogic Managed Server <p>See also, "Deploying WebCenter Portal: Framework Applications".</p>	Fusion Middleware Admin
Step 4 - Reconfigure back-end servers	<p>Reconfigure back-end server connections, if required, through Fusion Middleware Control.</p> <ul style="list-style-type: none"> ▪ Content Repositories <ul style="list-style-type: none"> ▪ Managing Content Repositories ▪ Mail Servers <ul style="list-style-type: none"> ▪ Managing the Mail Service ▪ BPEL Servers <ul style="list-style-type: none"> ▪ Managing the Worklist Service ▪ Collaboration Services <ul style="list-style-type: none"> ▪ Managing the Announcements and Discussions Services ▪ Managing the Instant Messaging and Presence Service ▪ Secure Enterprise Search <ul style="list-style-type: none"> ▪ Managing Oracle SES Search in WebCenter Portal ▪ Analytics Services <ul style="list-style-type: none"> ▪ Managing the Analytics Service ▪ Activity Graph Services <ul style="list-style-type: none"> ▪ Managing the Activity Graph Service 	Fusion Middleware Admin

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

Step	Documentation	Role
<ul style="list-style-type: none"> ■ Personalization Services ■ External Applications ■ Portlet Producers ■ Group Events, Links, Lists, Notes, and Tags 	<ul style="list-style-type: none"> ■ Managing Personalization for WebCenter Portal ■ Managing External Applications ■ Registering WSRP Producers ■ Registering Oracle PDK-Java Producers ■ Registering the Pagelet Producer ■ Setting Up Database Connections ■ Setting Up the MDS Repository 	
Step 5 - Connect to an identity store	<p>Ensure that your identity store is installed, configured, and contains all the required user data. See:</p> <ul style="list-style-type: none"> ■ Configuring the Identity Store <p>See also <i>Oracle Fusion Middleware Application Security Guide</i>.</p>	Fusion Middleware Admin
Step 6 - Restart the managed server	<p>Restart the managed server on which the application is deployed. See:</p> <ul style="list-style-type: none"> ■ Starting and Stopping Managed Servers for WebCenter Portal Application Deployments 	Fusion Middleware Admin
Step 7 - Verify Framework application configuration	<p>Login to the application to verify the configuration: identity store, services, applications, and so on.</p> <ul style="list-style-type: none"> ■ Using WebCenter Portal Administration Console 	Framework Application Admin
Step 8 - Perform administrative tasks through WebCenter Portal Administration pages	<p>Perform administrative duties:</p> <ul style="list-style-type: none"> ■ Set application-level preferences ■ Manage users and grant application roles ■ Manage and configure application resources ■ Manage and configure content ■ Manage and configure portlet producers ■ Manage and configure external applications ■ Create and manage polls <p>See: Using WebCenter Portal Administration Console</p>	Application Admin

Maintaining Framework Applications

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

- [Section 5.1, "System Administration for Framework Applications \(Roadmap\)"](#)

Although the Spaces application was built using WebCenter Portal: Framework, it does require some special maintenance tasks that Framework applications do not. To see a comprehensive list of these tasks, refer to [Chapter 3, "Maintaining the Spaces Application"](#).

Audience

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

5.1 System Administration for Framework Applications (Roadmap)

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

If the Framework 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 Framework Applications

Tasks	Documentation	Role
Stop and start the managed server	Restart the managed server on which the Framework application is deployed to effect configuration changes or for routine maintenance: <ul style="list-style-type: none"> ■ Starting and Stopping Managed Servers for WebCenter Portal Application Deployments 	Fusion Middleware Admin
Stop and start the Framework application	Shut down the application for maintenance purposes and then restart the application: <ul style="list-style-type: none"> ■ Starting and Stopping Framework Applications 	Fusion Middleware Admin
Maintain back-end services	Add, modify, and delete connections through the Fusion Middleware Control Console:	Fusion Middleware Admin

Table 5–1 (Cont.) Roadmap - Maintaining Framework Applications

Tasks	Documentation	Role
<ul style="list-style-type: none"> ■ Content Repositories ■ Mail Servers ■ BPEL Servers ■ Collaboration Services ■ Secure Enterprise Search ■ Analytics Services ■ Activity Graph Services ■ Personalization Services 	<ul style="list-style-type: none"> ■ Managing Content Repositories ■ Managing the Mail Service ■ Managing the Worklist Service ■ Managing the Announcements and Discussions Services ■ Managing the Instant Messaging and Presence Service ■ Managing Oracle SES Search in WebCenter Portal ■ Managing the Analytics Service ■ Managing the Activity Graph Service ■ Managing Personalization for WebCenter Portal 	
Maintain external applications and portlet producers	Add, modify, and delete connections through Oracle Enterprise Manager Fusion Middleware Control Console. See:	Fusion Middleware Admin
<ul style="list-style-type: none"> ■ External Applications ■ Portlet Producers 	<ul style="list-style-type: none"> ■ Managing External Applications ■ Registering WSRP Producers ■ Registering Oracle PDK-Java Producers ■ Registering the Pagelet Producer 	
Reassociate your identity, policy and credential stores	Reassociate your identity or policy stores: <ul style="list-style-type: none"> ■ Configuring the Identity Store ■ Configuring the Policy and Credential Store See also <i>Oracle Fusion Middleware Application Security Guide</i> .	Fusion Middleware Admin
Reconfigure the MDS repository	<ul style="list-style-type: none"> ■ Setting Up the MDS Repository 	Fusion Middleware Admin
Reconfigure WebCenter Portal repository	<ul style="list-style-type: none"> ■ Setting Up Database Connections 	
Export Framework application data	Migrate data to a remote instance or between stage and production environments: <ul style="list-style-type: none"> ■ Exporting WebCenter Portal Service Metadata and Data (Framework Applications) ■ Exporting Portlet Client Metadata (Framework Applications) ■ Migrating Security for WebCenter Portal Applications ■ Migrating Data (WebCenter Portal Applications) See also, "Managing Export, Import, Backup, and Recovery of WebCenter Portal".	Fusion Middleware Admin

Table 5–1 (Cont.) Roadmap - Maintaining Framework Applications

Tasks	Documentation	Role
Import Framework application data	Use the import facility to move content to a remote instance or between stage and production environments: <ul style="list-style-type: none"> ▪ Importing WebCenter Portal Service Metadata and Data (Framework Applications) ▪ Importing Portlet Client Metadata (Framework Applications) ▪ Migrating Security for WebCenter Portal Applications ▪ Migrating Data (WebCenter Portal Applications) 	Fusion Middleware Admin
View and manage log files	Identify and diagnose problems through log files. Framework application logs record all types of events, including startup and shutdown information, errors, warnings, and other information: <ul style="list-style-type: none"> ▪ Viewing and Configuring Log Information 	Fusion Middleware Admin
Monitor performance	Analyze the performance of the Framework application and monitor its current status through Fusion Middleware Control Console: <ul style="list-style-type: none"> ▪ Viewing Performance Information ▪ Monitoring Framework Applications 	Fusion Middleware Admin
Tune application properties	Reconfigure performance related parameters for the WebCenter Portal environment, application, and services: <ul style="list-style-type: none"> ▪ Tuning Oracle WebCenter Portal Performance 	Fusion Middleware Admin
Perform application administrative tasks through WebCenter Portal Administration pages	Perform application administrative duties: <ul style="list-style-type: none"> ▪ Set application-level preferences ▪ Manage users and grant application roles ▪ Manage and configure application resources ▪ Manage and configure content ▪ Manage and configure portlet producers ▪ Manage and configure external applications ▪ Create and manage polls See: Using WebCenter Portal Administration Console	Application Admin

Part III

Basic Systems Administration for Oracle WebCenter Portal

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

Part III contains the following chapters:

- [Chapter 6, "Starting Enterprise Manager Fusion Middleware Control"](#)
- [Chapter 7, "Deploying WebCenter Portal: Framework Applications"](#)
- [Chapter 8, "Starting and Stopping WebCenter Portal Applications"](#)
- [Chapter 9, "Setting WebCenter Portal Application Properties"](#)

Starting Enterprise Manager Fusion Middleware Control

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

This chapter includes the following sections:

- [Section 6.1, "Displaying Fusion Middleware Control Console"](#)
- [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
- [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
- [Section 6.4, "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 pages for managing WebCenter Portal. Your role determines what you can see and do after logging in. To find out more, see [Table 1-7, "WebCenter Portal 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.

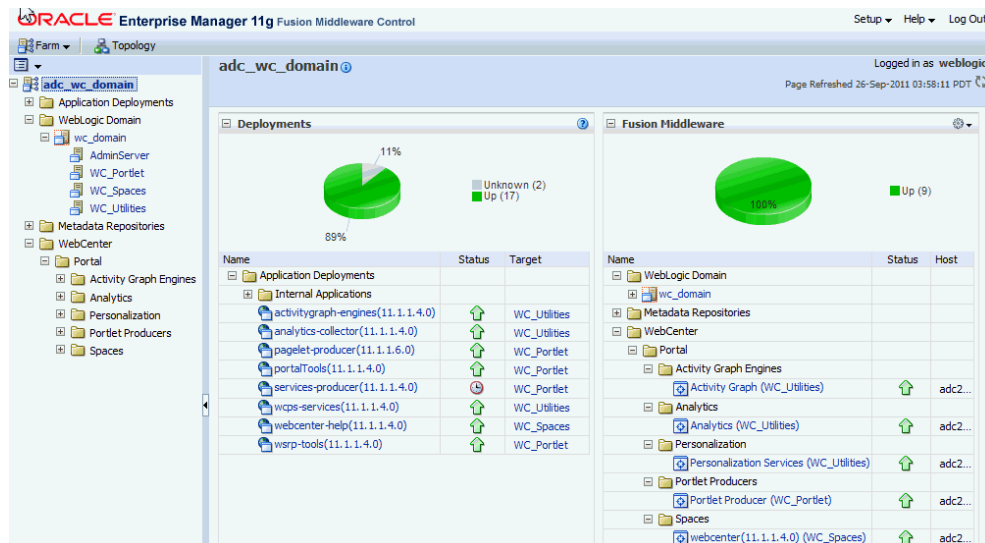
The default user name for the administrator user is `weblogic`. This is the account you can use to log in to Fusion Middleware Control for the first time.

4. Click **Login**.

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

Tip: If you are unable to log in, try logging in to the WebLogic Admin Console to confirm your host/port/credentials. The Weblogic Admin Console is accessible at the same host/port as Fusion Middleware Control:
`http://host_name.domain_name:port_number/console`

Figure 6–1 Farm Home Page



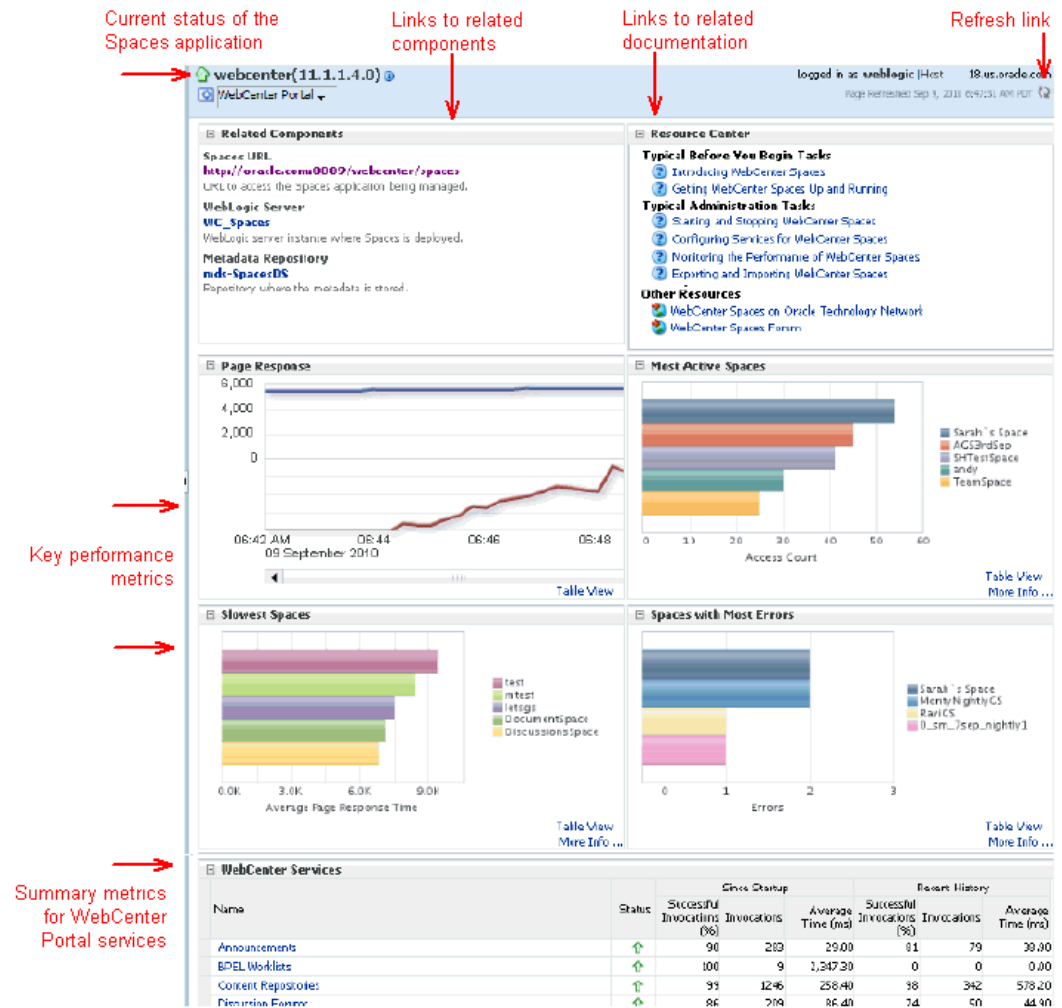
From the navigation pane, you can drill down to view and manage all components in your farm, including the Spaces application and any Framework application that you may have deployed. For detailed instructions, see:

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

6.2 Navigating to the Home Page for the Spaces Application

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

Figure 6–2 Spaces Home Page

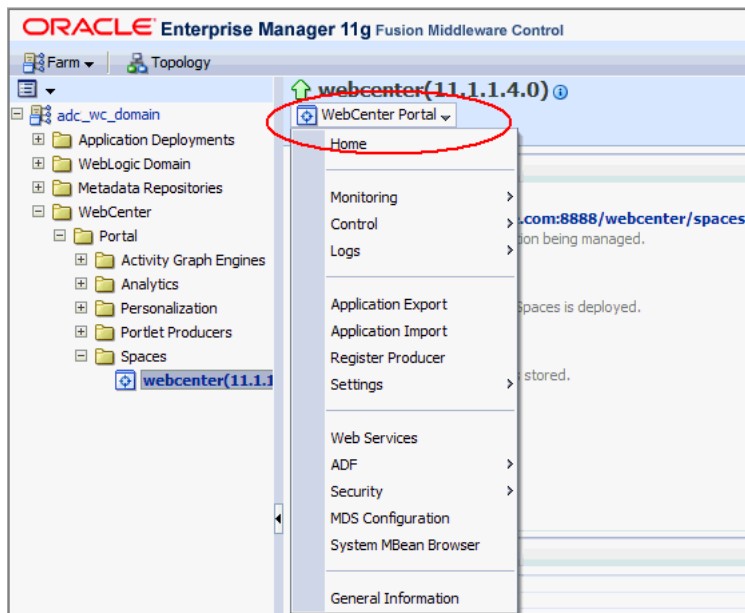


From here you can:

- Check the status of the Spaces application.
- View key space-related performance data. Track overall response time compared with the user access rate to see how the application performs under different loads and to diagnose system resource issues. Quickly see which spaces are used the most, the slowest performers, and determine which spaces are recording the most errors.
- Navigate to other key components, including the WebLogic Server installation, and the MDS repository.
- View status and key performance metrics for WebCenter Portal services used in the application.
- Drill down to detailed performance information for individual spaces, services, external applications, portlets, and producers.

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

Figure 6–3 WebCenter Portal Menu for the Spaces Application



From the WebCenter Portal menu, you can:

- Start and stop the Spaces application
- Configure application settings
- Manage back-end services
- Manage external applications
- Register and manage portlet producers
- Monitor detailed performance metrics for all components
- Select and chart live metrics
- Analyze diagnostic information and configure logs
- Export and import the Spaces application
- Configure security policies and roles.
- Configure ADF and MDS options.
- View Web Services-related information.

To navigate to the main home page for Spaces:

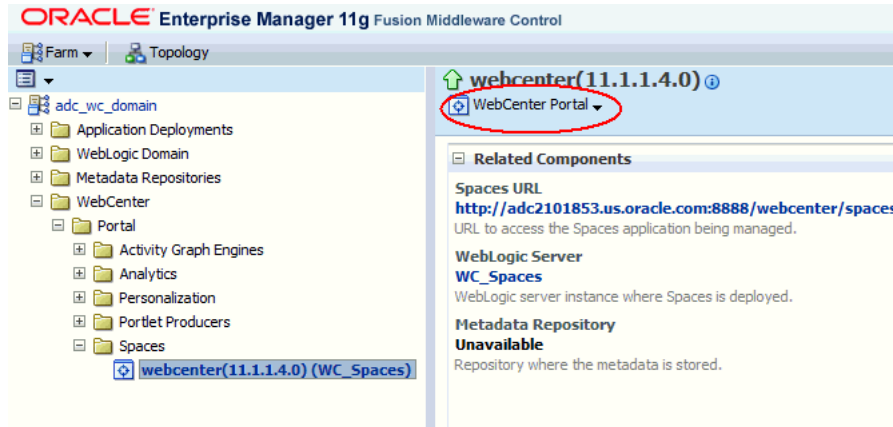
1. Login to Fusion Middleware Control.
See [Section 6.1, "Displaying Fusion Middleware Control Console"](#).
2. In the Navigator ([Figure 6–4](#)), expand **WebCenter > Portal > Spaces**.
3. Select **webcenter** to navigate to the home page for your Spaces installation ([Figure 6–4](#)).

Figure 6–4 Navigating to the Spaces Home Page



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

Figure 6–5 Displaying the Spaces Home Page and Menu



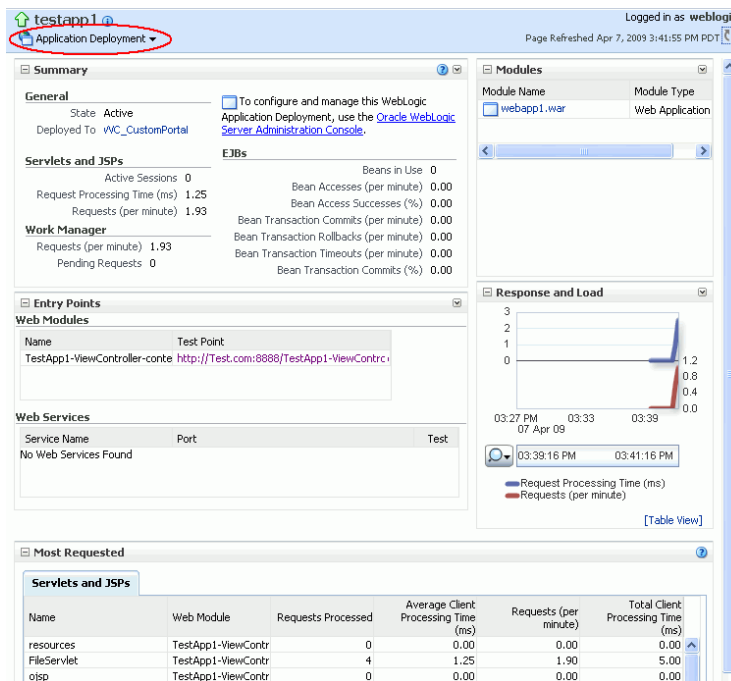
Another way to access the context menu for a particular component is to right-click the node in the navigation tree. For example, if you right-click the **Spaces** node on the left **webcenter(11.1.1.4.0)** the same *WebCenter Portal* menu displays.

6.3 Navigating to the Home Page for Framework Applications

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

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

Figure 6–6 Framework Application Home Page



From here you can:

- Check Framework 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 Framework application.
- Drill down to detailed performance information for individual modules and services.

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

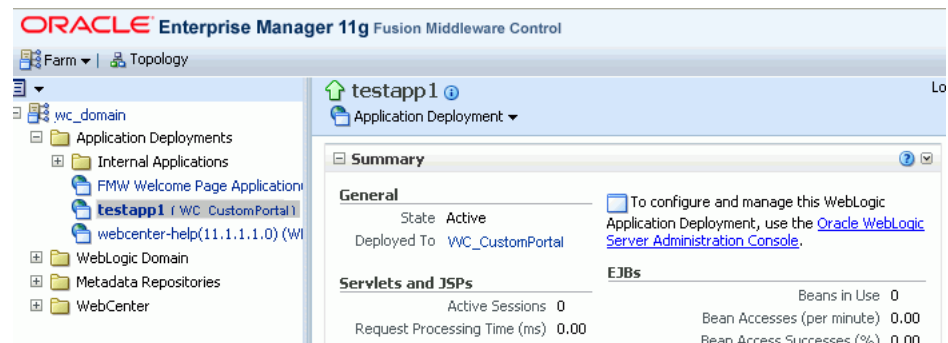
- Manage external applications (see [Chapter 26, "Managing External Applications"](#)).
- Manage back-end services (see [Chapter 10, "Managing Oracle WebCenter Portal Services"](#)).
- Manage portlet producers (see [Chapter 24, "Managing Portlet Producers"](#)).

- Monitor detailed performance metrics for WebCenter services (see [Chapter 38, "Monitoring Oracle WebCenter Portal Performance"](#)).

To navigate to the main home page for your Framework 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**.

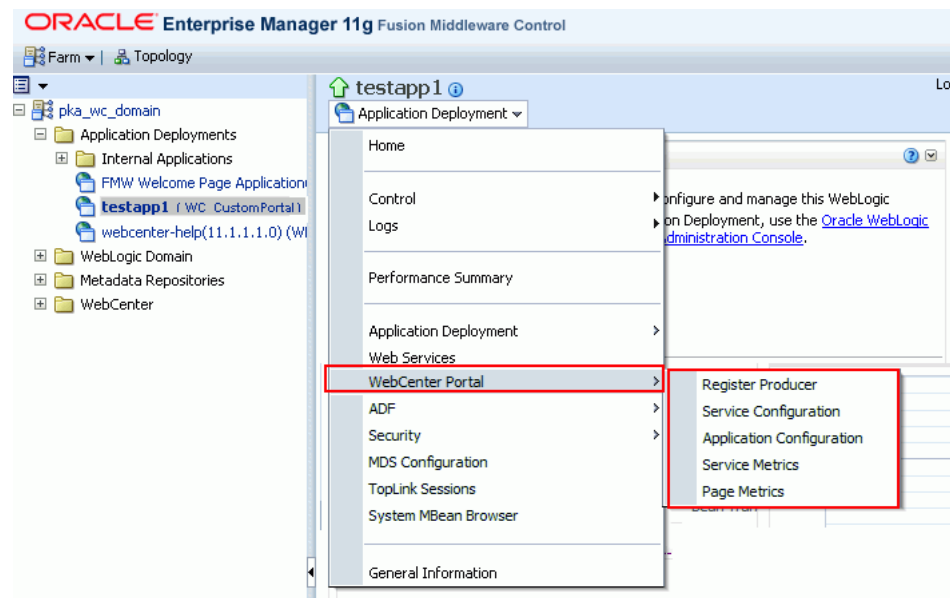
Figure 6-7 Navigating to a Framework Application Home Page



3. Select the name of your Framework application to display the application's home page.

Notice that WebCenter Portal menu options display on the **Application Deployment** menu ([Figure 6-8](#)).

Figure 6-8 Displaying the Framework Application Home Page and Menu



6.4 Navigating to Dependent Components

From WebCenter Portal 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.

- **Spaces application** - From the home page, click links in "Related Components" to navigate to Spaces application itself, WebLogic Server installation pages, and MDS repository pages in Fusion Middleware Control. See also, [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#).
- **Framework applications** - The Application Deployment menu on the J2EE application home page offers direct navigation to the Oracle WebLogic Server Administration Console, and pages relating to WebCenter Portal, ADF, MDS repository, and security configuration and administration. See also, [Section 6.3, "Navigating to the Home Page for Framework Applications"](#).

Deploying WebCenter Portal: Framework Applications

This chapter provides instructions for deploying, undeploying, and redeploying WebCenter Portal: Framework 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 Portal*).

This chapter does not contain instructions for deploying or installing the Spaces application. For information about installing Spaces and other WebCenter Portal components, see "Installing Oracle WebCenter Portal" in the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Portal*. For information about deploying WSRP and PDK-Java portlet producer applications, see [Section 24.8, "Deploying Portlet Producer Applications."](#)

This chapter includes the following sections:

- [Section 7.1, "Deploying Framework applications"](#)
- [Section 7.2, "Undeploying Framework applications"](#)
- [Section 7.3, "Redeploying Framework applications"](#)
- [Section 7.4, "Post-Deployment Configuration"](#)

Audience

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

7.1 Deploying Framework applications

This section describes the steps required to deploy a Framework application created in JDeveloper to a production domain. The deployment steps in this section assume that you are deploying an EAR file, know its location, and that the domain to which you want to deploy exists.

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

This section includes the following topics:

- [Section 7.1.1, "Deployment Roadmap"](#)

- Section 7.1.2, "Deployment Prerequisites"
- Section 7.1.3, "Preparing the Application EAR File"
- Section 7.1.4, "Creating a Managed Server"
- Section 7.1.5, "Creating and Registering the Metadata Service Repository"
- Section 7.1.6, "Deploying the Application to a WebLogic Managed Server"
- Section 7.1.7, "Migrating Customizations and Data Between Environments"
- Section 7.1.8, "Configuring Applications to Run in a Distributed Environment"

7.1.1 Deployment Roadmap

The flow chart and table in this section provide an overview of the prerequisites and tasks required to deploy a Framework application to an Oracle WebLogic Managed Server. Figure 7-1 shows the steps to deploy a Framework application, and the roles that will carry them out.

Figure 7-1 Deploying a Framework application to a Managed Server

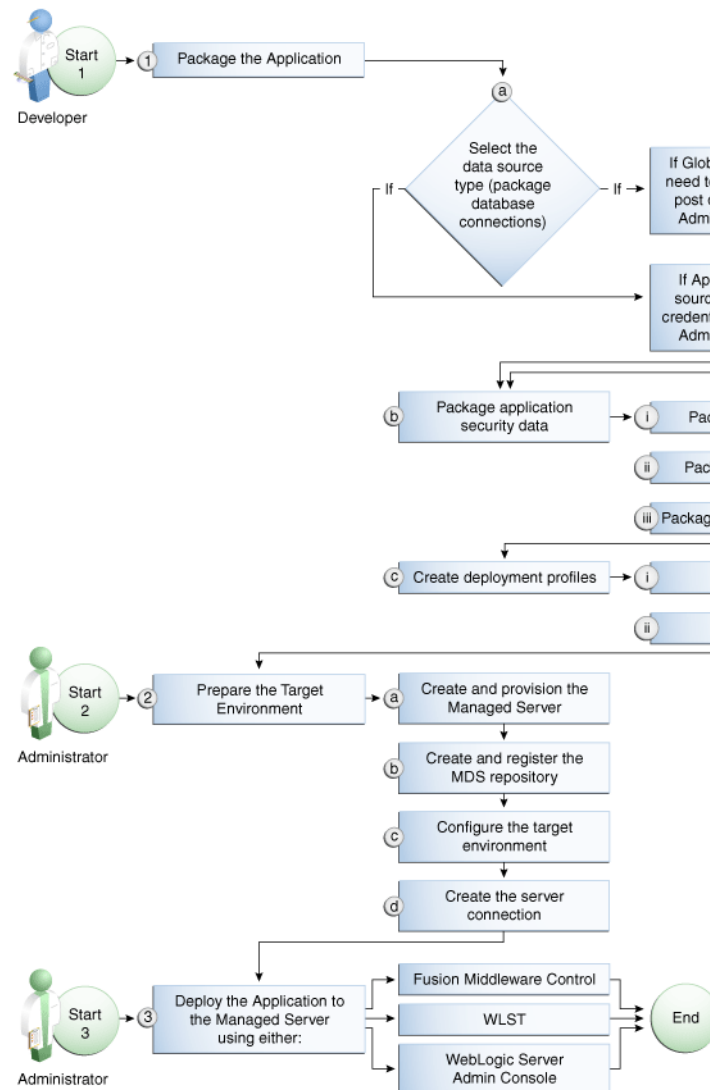


Table 7–1 shows the tasks, sub-tasks and who will need to carry them out to deploy a Framework application from JDeveloper.

Table 7–1 Deploying a Framework application to a Managed Server

Actor	Task	Sub-task	Notes
Developer	1. Package the Application	1.a Select the data source type (package database connections)	You can use either a global data source or an application-level data source. If using a global data source, then you need to create the data source in the WLS Administration Console before deploying. If using an application-level data source, then you need to add credential mappings in the WLS Administration Console after deploying.
		1.b Package application security data	This sub-task consists of packaging the credentials, identity data, and application policies.
		1.c Create deployment profiles	This sub-task consists of creating the WAR and EAR files.
Administrator	2. Prepare the Target Environment	2.a Create and provision the Managed Server	
		2.b Create and register the MDS repository	
		2.c Configure the target environment	
		2.d Create the server connection	
Developer	3. Deploy the Application to a Managed Server		The final step is to deploy the application to the Managed Server using either Fusion Middleware Control, WLST, or the WLS Admin Console.

7.1.2 Deployment Prerequisites

You can deploy Framework applications to any WebLogic Managed Server instance that is provisioned with the Oracle WebCenter Portal libraries.

Note: Oracle does not recommend deploying Framework applications to any of the preconfigured Managed Servers created during the installation, or to the Administration Server. For Framework applications, follow the process described in "Extending an Existing Domain" in the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Portal* to create and provision a new WLS Managed Server before deploying. For portlet producer applications, you can optionally create a new WebLogic Managed Server or deploy to the WC_Portlet server.

Before deploying, you must:

- Prepare the application EAR file, as described in [Section 7.1.3, "Preparing the Application EAR File."](#)

- Create a WebLogic Managed Server, as described in [Section 7.1.4, "Creating a Managed Server."](#)
- Create and register a Metadata Service (MDS) repository, as described in [Section 7.1.5, "Creating and Registering the Metadata Service Repository."](#)

Note: You must delete runtime customizations (customizations not done through JDeveloper) before deploying an updated application that has had major changes to artifacts such as pages, connections, or task flows.

After completing these steps, continue by deploying the application as described in [Section 7.1.6, "Deploying the Application to a WebLogic Managed Server."](#)

7.1.3 Preparing the Application EAR File

Before you deploy an application, you must first create a deployment profile. The deployment profile packages or archives the Framework application and its associated files so that the application can be deployed to an Oracle WebLogic Managed Server as an EAR file.

For information on how to create a deployment profile (and the resulting EAR file) for an application, see "Packaging and Deploying a Framework Application to a WebLogic Managed Server" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

7.1.3.1 EAR File Contents

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 Framework application.

7.1.4 Creating a Managed Server

Before deploying a Framework application, you must create a WebLogic Managed Server based on the "Oracle WebCenter Portal Framework" template that contains all the required shared libraries and a MDS Repository. If a Framework application has been portletized it should be deployed to the Oracle WebCenter Portal Custom Services Producer server (`WC_CustomServicesProducer`). A portletized application cannot be deployed to the Oracle WebCenter Portal Custom Portal server as it lacks the required portlet libraries. Note that the Oracle WebCenter Portal Custom Services Producer and Oracle WebCenter Portal Custom Portal servers have not only the MDS schema targeted to them but also WebCenter Portal and Activities.

For instructions on how to create a new managed server, see "Extending an Existing Domain" in the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Portal*.

For instructions on how to create a new domain, see "Creating a New Domain" in the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Portal*.

7.1.5 Creating and Registering the Metadata Service Repository

Before deploying an application to a Managed Server, you may need to create and register a Metadata Service (MDS) repository schema for the application on the WebLogic Domain's Administration Server instance. The target server (Oracle WebCenter Portal Custom Portal server or Oracle WebCenter Portal Custom Services Producer server) already has the MDS data source configured, so this step is only required if you do not want to use the pre-configured server MDS data source. Do not, however, create a new MDS schema if it is being shared by other applications.

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

At deployment time, some configuration information and application metadata exported into the EAR file must 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 7.1.6, "Deploying the Application to a WebLogic Managed Server"](#)).

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

This section contains the following subsections:

- [Section 7.1.5.1, "Creating an MDS Schema Using the Repository Creation Utility"](#)
- [Section 7.1.5.2, "Registering an MDS Schema Using Fusion Middleware Control"](#)
- [Section 7.1.5.3, "Registering an MDS Schema Using WLST"](#)

7.1.5.1 Creating an MDS Schema Using the Repository Creation Utility

Before you deploy an application, you must first create the MDS schema on a database server instance using the Repository Creation Utility (RCU), 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 need this information for subsequent steps in the deployment process.

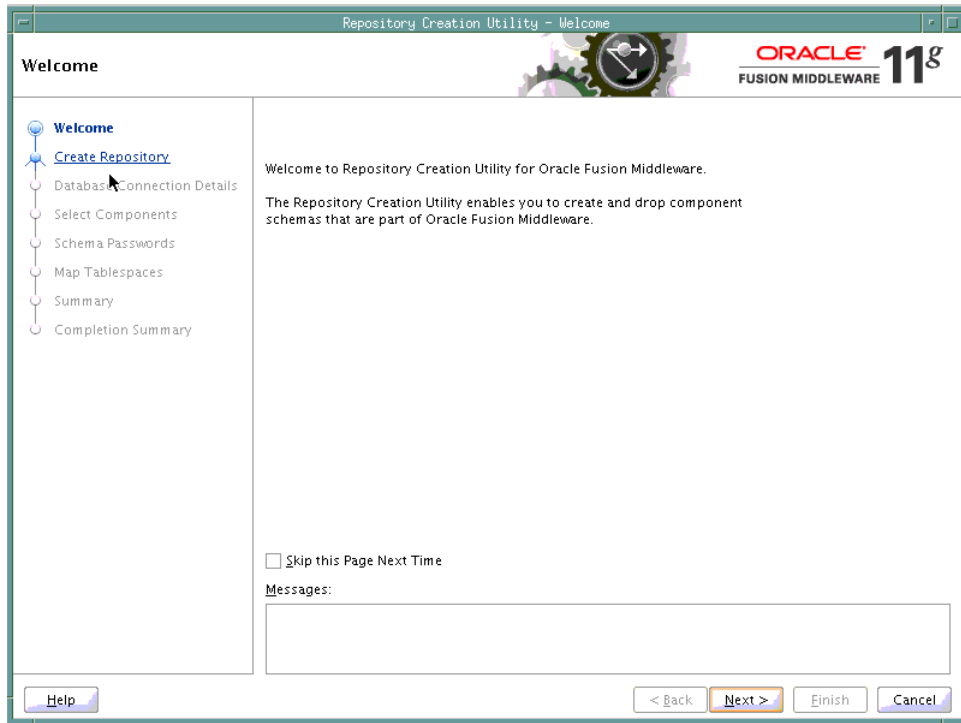
To create the MDS schema:

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

```
rcu
```

The RCU Welcome page displays (see [Figure 7-2](#)).

Figure 7-2 RCU Welcome Page



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

The Database Connection Details page displays (see [Figure 7-3](#)).

Figure 7-3 Database Connection Details Page

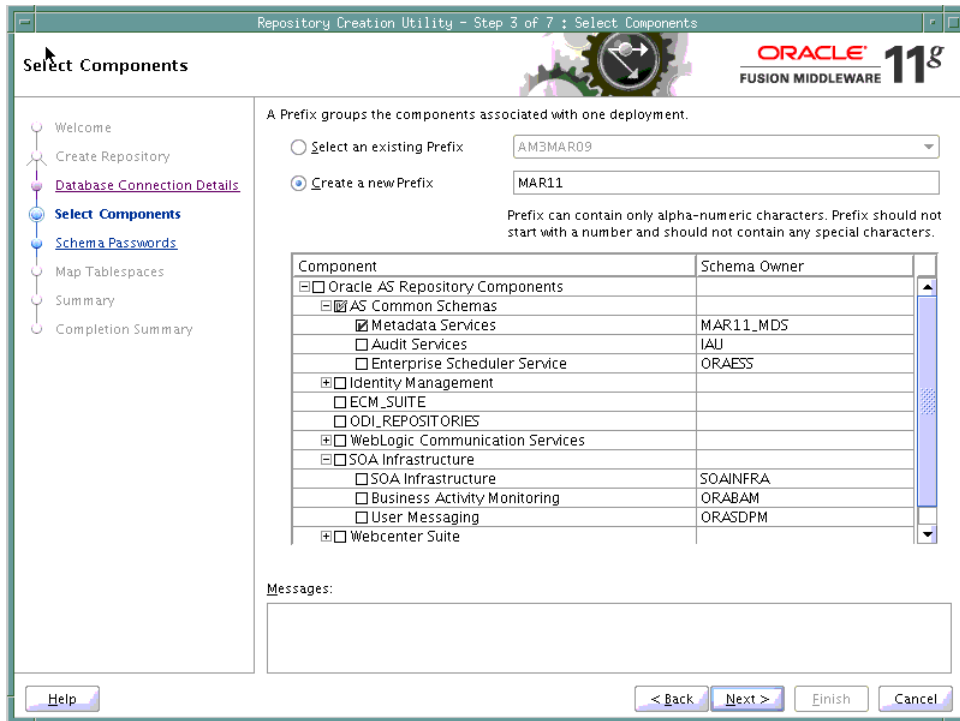
The screenshot shows the 'Database Connection Details' page in the Oracle Fusion Middleware 11g Repository Creation Utility. The window title is 'Repository Creation Utility - Step 2 of 7 : Database Connection Details'. The page has a navigation pane on the left with the following steps: Welcome, Create Repository, Database Connection Details (highlighted), Select Components, Schema Passwords, Map Tablespaces, Summary, and Completion Summary. The main content area contains the following fields:

- Database Type:** Oracle Database (selected in a dropdown menu)
- Host Name:** (text input field) with a note: 'For RAC database, specify VIP name or one of the Node name as Host name.'
- Port:** (text input field)
- Service Name:** (text input field)
- Username:** (text input field)
- Password:** (text input field)
- Role:** SYSDBA (selected in a dropdown menu) with a note: 'One or more components may require SYSDBA role for the operation to succeed.'

At the bottom, there is a 'Messages:' section with a text area and a 'Help' button. The bottom right corner contains navigation buttons: '< Back', 'Next >', 'Finish', and '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 7-4](#)).

Figure 7-4 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 7-5](#)).

Figure 7–5 Schema Passwords Page

Repository Creation Utility – Step 4 of 7 : Schema Passwords

Schema Passwords

Please enter the passwords for the main and additional (auxiliary) schema users. Password can contain alphabets, numbers and the following special characters: \$, #, _

Use same passwords for all schemas
 Use main schema passwords for auxiliary schemas
 Specify different passwords for all schemas

Component	Schema Owner	Schema Password	Confirm Password
Metadata Services	MAR11_MDS	*****	*****

Messages:

Help < Back Next > Finish Cancel

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**.

7.1.5.2 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 7–6](#)).

Figure 7–6 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	

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

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

Figure 7–7 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:

6. 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.

7.1.5.3 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 1.13.3.1, "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 fully qualified server name of the database server 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 the 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')
```

7.1.6 Deploying the Application to a WebLogic Managed Server

For Framework applications created in JDeveloper, follow the process described in "Extending an Existing Domain" in the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Portal* to create and provision a new Oracle WebCenter Portal Custom Portal server, or if portletized, Oracle WebCenter Portal Custom Services Producer server before deploying.

Table 7–2 Deployment Targets

Application Type	Managed Server Name
Framework applications	WC_CustomPortal
WebCenter Portal Portlet Producer applications	WC_CustomServicesProducer
Non-WebCenter Portal Portlet Producer applications	WC_Portlet For portlet producer applications, you can either create a Managed Server instance or deploy to the WC_Portlet server.

Note: Oracle does not recommend deploying Framework applications to any of the preconfigured Managed Servers created during the installation, or to the Administration Server.

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

- [Section 7.1.6.1, "Choosing the Information Artifact Store"](#)
- [Section 7.1.6.2, "Choosing the Data Source"](#)
- [Section 7.1.6.3, "Deploying Applications Using Oracle JDeveloper"](#)
- [Section 7.1.6.4, "Deploying Applications Using Fusion Middleware Control"](#)
- [Section 7.1.6.5, "Deploying Applications Using WLST"](#)
- [Section 7.1.6.6, "Deploying Applications Using the WLS Administration Console"](#)
- [Section 7.1.6.7, "Saving and Reusing the Deployment Plan"](#)

7.1.6.1 Choosing the Information Artifact Store

As explained in [Section 7.1.3, "Preparing the Application EAR File,"](#) the packaged EAR file consists of several information artifacts, which includes the application binaries, the application configuration, the application metadata, and the portlet customizations.

During the deployment, these information artifacts must 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 7–3:](#)

Table 7–3 Information Artifact Target Stores

Information Artifact	Target Information Store
Application Binaries	Target Server Instance
Application Configuration	MDS
Application Metadata	MDS
Portlet Customizations	Target Producer

Regardless of the tool you choose to deploy, you must supply the target information store locations for correct deployment. The application deployment fails if the MDS location is incorrect or not supplied. The application will still deploy, however, if the target producer is incorrectly specified. If you incorrectly specify the target producer, the portlets are not imported automatically and, consequently, are not operational. If that happens, do one of the following:

- Edit the portlet producers connections post-deployment using Fusion Middleware Control (see [Section 24.2.1, "Registering a WSRP Producer Using Fusion Middleware Control"](#) and [Section 24.4.1, "Registering an Oracle PDK-Java Producer Using Fusion Middleware Control"](#)) or WLST commands (see [Section 24.2.2, "Registering a WSRP Producer Using WLST"](#) or [Section 24.4.2, "Registering an Oracle PDK-Java Producer Using WLST"](#)), and redeploy the application.
- Export and import the portlet customization using WLST commands (see [Section 39.2, "Exporting and Importing Framework Applications for Data Migration"](#)).

Note: If the application is deployed and the target producer is incorrectly specified but the target exists, the portlets are imported but to the wrong producer and the portlets are not operational.

7.1.6.2 Choosing the Data Source

There are three basic options for data sources:

- Deploying to a WebCenter Portal Custom Portal Managed Server using pre-existing data sources
- Deploying to a Managed Server using global data sources not named WebCenterDS or ActivitiesDS
- Deploying to a Managed Server using local application context data sources of any name

This section describes the benefits and drawbacks of each of these options:

Deploying to a WebCenter Portal Custom Portal Managed Server using pre-existing data sources

This option requires the least effort in enabling a Framework application to access the required data sources, and is the recommended deployment path.

To deploy using pre-existing data sources, deselect the **Auto Generate and Synchronize weblogic-jdbc.xml Descriptors During Deployment** check box on the the Application Properties Deployment screen in JDeveloper.

If your application has existing database connections configured for WebCenterDS and/or ActivitiesDS and these are not named "webcenter/CustomPortal" and

"activities/CustomPortal" respectively, either the database connections should be deleted from the application prior to deployment, or the database connections should be created and named following the naming convention.

Deploying to a Managed Server using global data sources not named WebCenterDS or ActivitiesDS

Use this deployment path when the application is not intended to run on a Managed Server created with the Oracle WebCenter Custom Portal template, or is intended to run against custom data sources not named "WebCenterDS" or "ActivitiesDS".

For this option the Framework application should have had database connections created and associated as either the `WEBCENTER` or `ACTIVITIES` schema. The **Auto Generate and Synchronize weblogic-jdbc.xml Descriptors During Deployment** check box on the Application Properties Deployment screen in JDeveloper should be deselected. The global data sources intended to be used on the WLS server requires them to be created with the JNDI names matching those of the database connections created for the application in the JDeveloper project. For more information, see *Creating a JDBC Data Source* on OTN.

Deploying to a managed server using local application context data sources of any name

Use this deployment path if the application local context data sources are sufficient.

This choice requires only that the Framework application has a database connection created for and associated with `WebCenterDS` and/or `ActivitiesDS` (depending on which services are being used in the application). The Application Properties Deployment screen in JDeveloper should have the **Auto Generate and Synchronize weblogic-jdbc.xml Descriptors During Deployment** check box selected.

7.1.6.3 Deploying Applications Using Oracle JDeveloper

You can deploy Framework applications to a WebLogic server instance directly from a development environment using Oracle JDeveloper, if you have the necessary credentials to access the WebLogic server. For more information, see "Creating a WebLogic Managed Server Connection" and "Deploying a Framework application to a Managed Server" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

7.1.6.4 Deploying Applications Using Fusion Middleware Control

When deploying a Framework application using Fusion Middleware Control you must know the location of the application archive, and whether a deployment plan exists for the application. See [Section 7.1.6.7, "Saving and Reusing the Deployment Plan"](#) for more information about deployment plans.

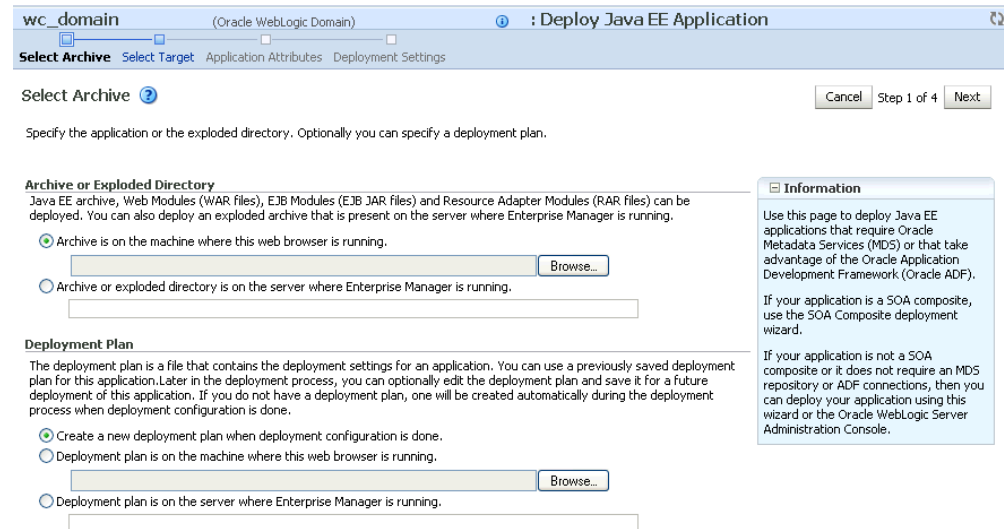
Note: Metadata repository and ADF connection details specified during deployment are not stored as part of the deployment plan. You will need to specify these deployment properties each time you deploy the application.

If you plan on updating and deploy the application frequently and want to maintain these configuration changes, it is recommended that you make those configuration changes post-deployment using WLST or Fusion Middleware Control. Such configuration changes are saved in the deployment plan and persisted in the MDS repository and do not need to be set again when you redeploy the application.

To deploy a Framework application using Fusion Middleware Control:

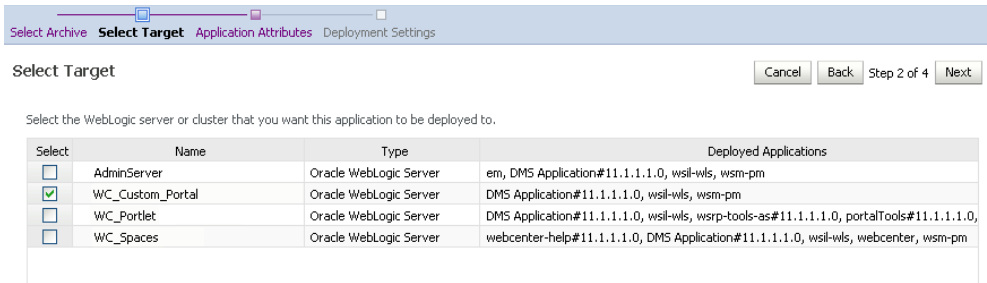
1. Log in to Fusion Middleware Control.
See [Section 6.1, "Displaying Fusion Middleware Control Console."](#)
2. In the Navigation pane, expand **WebLogic Domain** and click the domain in which your target Managed Server was created.
3. From the WebLogic Domain menu, select **Application Deployment > Deploy**.
The Select Archive page displays (see [Figure 7–8](#)).

Figure 7–8 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 7–9](#)).

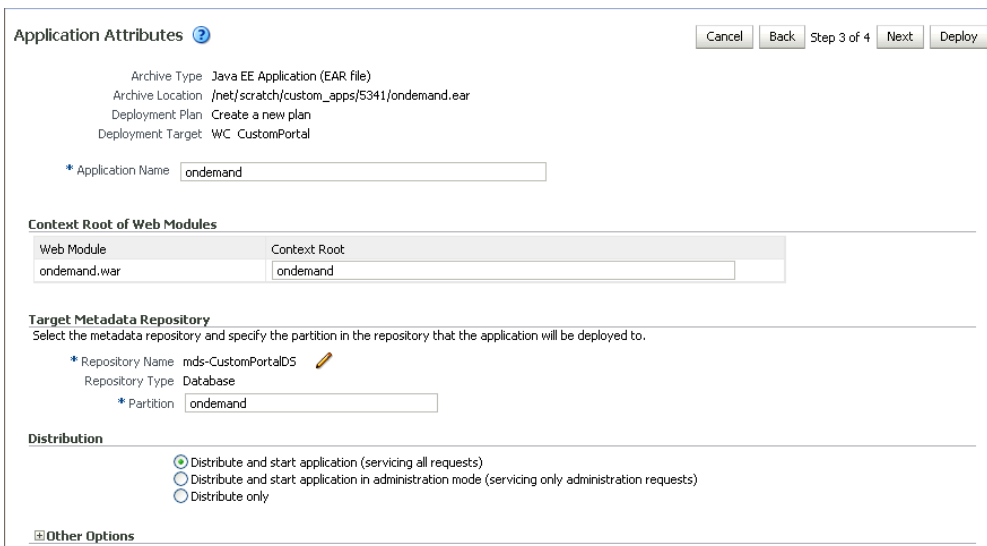
Figure 7–9 Select Target Page



7. Select the target server(s) to deploy the application to (see [Section 7.1.6, "Deploying the Application to a WebLogic Managed Server"](#) for an overview of selecting the targets) and click **Next**.

The Application Attributes page displays (see [Figure 7–10](#)).

Figure 7–10 Application Attributes Page



8. 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 7–11](#). 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 7–11 Select Metadata Repository Window

Metadata Repositories

Select the metadata repository that the application will be deployed to.

Repository: mds-CustomPor

Repository Details

Name: mds-CustomPortalDS
 Type: Database
 JNDI Location: jdbc/mds/CustomDS
 Database Type: Oracle
 Database Name: db6529
 Database User: DADVM427_MDS
 JDBC URL: jdbc:oracle:thin:example.com:1521:db6529

OK Cancel

9. 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.

10. Click Next.

The Deployment Settings page displays (see [Figure 7–12](#)).

Figure 7–12 Deployment Settings Page

Deployment Settings

Cancel Back Step 4 of 4 Deploy

Archive Type: Java EE Application (EAR file) Application Name: ondemand
 Archive Location: /net/example/scratch/custom_apps/5341/ondemand.ear Version: V2.0
 Deployment Plan: Create a new plan Context Root: ondemand
 Deployment Target: WC_CustomPortal Deployment Mode: Distribute and start application (servicing all requests)

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

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 deployed.

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

Edit Deployment Plan

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.

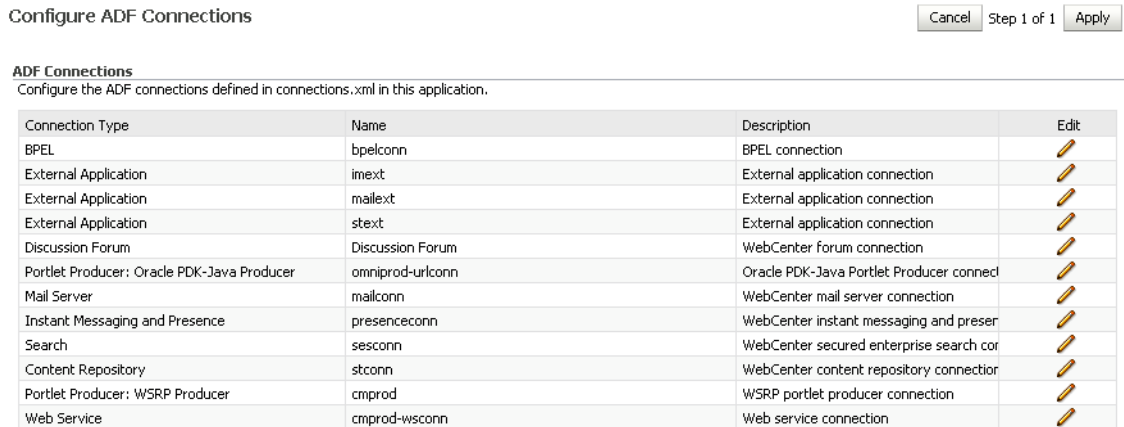
Save Deployment Plan

You have now provided the Target MDS location (described in [Section 7.1.6, "Deploying the Application to a WebLogic Managed Server"](#)).

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

The Configure ADF Connections page displays (see [Figure 7–13](#)).

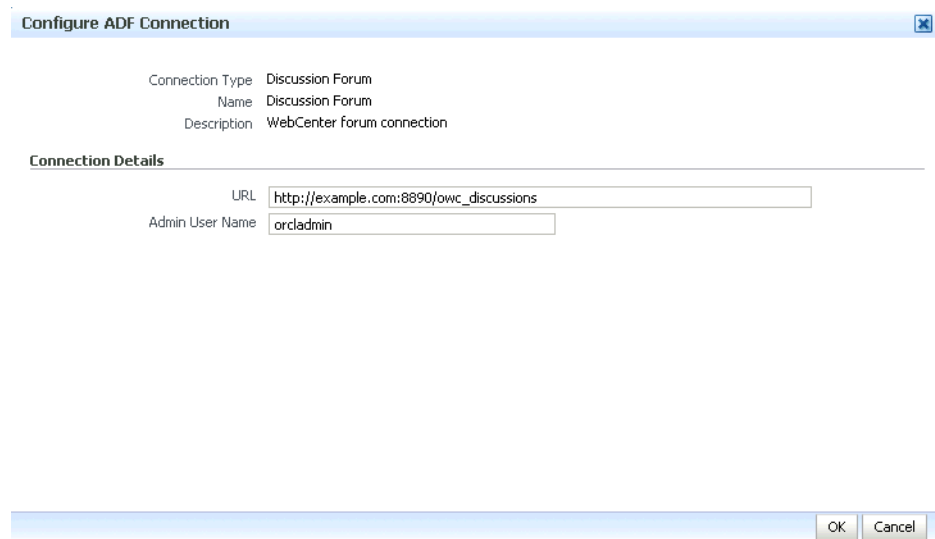
Figure 7–13 Configure ADF Connections Page



- 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 7–14](#)), for example, ensure that the URL to the Discussions server, and the user account used to connect to the server are correct for the target environment.

Figure 7–14 Discussion Forum Connection Settings



For WSRP producers, two connections are shown for each producer: a WSRP Producer and a Web Service connection. Typically only the Web Service connection must be changed to the target producer, and this contains four URL endpoints, all of which must 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 must 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 7.1.6, "Deploying the Application to a WebLogic Managed Server"](#).

Note: If any target producers are not reachable as the application starts for the first time, the import fails. After the portlet producer becomes reachable, restart the application and try to import again.

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), portlets are imported to the incorrect producers.

To remedy, after deployment use Fusion Middleware Control (see [Section 24.2.1, "Registering a WSRP Producer Using Fusion Middleware Control"](#) and [Section 24.4.1, "Registering an Oracle PDK-Java Producer Using Fusion Middleware Control"](#)) or WLST commands (see [Section 24.2.2, "Registering a WSRP Producer Using WLST"](#) or [Section 24.4.2, "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 Framework 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. In the Deployment Plan section, click **Edit Deployment Plan** to optionally edit the currently selected Deployment Plan.
15. In the Deployment Plan section, click **Save Deployment Plan** to optionally save the currently selected Deployment Plan for reuse when you redeploy the application.
16. To start the deployment process, click **Deploy**.
Fusion Middleware Control displays processing messages.
17. Click **Close** in the Deployment Succeeded page.
The Framework application (and its deployment plan) is now deployed on the WebLogic Managed Server instance.
18. 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: If you configured connections during deployment these are not stored as part of the deployment plan. You must specify these connection details again the next time you deploy.

7.1.6.5 Deploying Applications Using WLST

To deploy a Framework 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 Framework application using WLST:

1. Start the WLST shell.

For information on starting the WLST shell, see [Section 1.13.3, "Oracle WebLogic Scripting Tool \(WLST\)."](#)

2. Connect to the Administration Server of your WebCenter Portal 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*.

4. After retrieving the MDS configuration information from the EAR file, you must set the proper MDS schema information according to your WebCenter Portal 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/feb23demo*)
5. After setting the MDS repository information, save function the MDS configuration information with the following command:

```
archive.save()
```

6. Deploy the Framework application using the WLST deploy command.

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

Where:

- *appName* is the name of the Framework 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 starts automatically.

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

To remedy this, after deployment, use Fusion Middleware Control (see [Section 24.2.1, "Registering a WSRP Producer Using Fusion Middleware Control"](#) and [Section 24.4.1, "Registering an Oracle PDK-Java Producer Using Fusion Middleware Control"](#)) or WLST commands (see [Section 24.2.2, "Registering a WSRP Producer Using WLST"](#) or [Section 24.4.2, "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 Framework Applications Using Fusion Middleware Control."](#)

7.1.6.6 Deploying Applications Using the WLS Administration Console

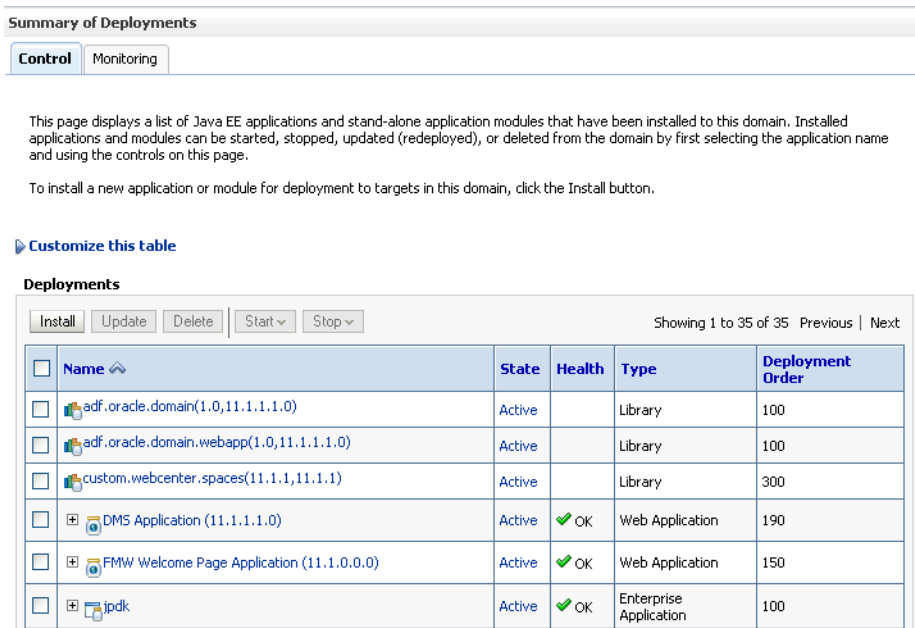
You can use the WLS Administration Console to deploy a Framework application or a portlet producer application. However, the Console does not offer a means to change ADF connections, including the essential MDS connection. To use the Console to deploy a Framework application, the MDS connection in the EAR file must be configured to the target deployment repository. Follow steps 1-5 in [Section 7.1.6.5, "Deploying Applications Using WLST,"](#) then follow the steps below to deploy a Framework application or portlet producer application using the WLS Administration Console.

Note: Oracle does not recommend deploying Framework applications to any of the preconfigured Managed Servers created during the installation, or to the Administration Server. For Framework applications created in JDeveloper, follow the process described in "Extending an Existing Domain" in the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Portal* to create and provision a new WLS Managed Server before deploying. For portlet producer applications, you can create a Managed Server instance, or optionally deploy to the WC_Portlet server.

To deploy a Framework application 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 1.13.2, "Oracle WebLogic Server Administration Console."](#)
2. In the Domain Structure pane, click **Deployments**.
 The Deployments Summary pane displays (see [Figure 7–15](#)).

Figure 7–15 Deployment Summary Pane



3. On the Deployment Summary pane, click **Install**.
 The Install Application Assistant page displays (see [Figure 7–16](#)).

Figure 7–16 Install Application Assistant Page

- 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 7–17](#)).

Figure 7–17 Install Application Assistant - Page 2

- Select **Install this deployment as an application** (for both Framework applications and portlet producers) and click **Next**.

Page 3 of the Install Application Assistant displays (see [Figure 7–18](#)).

Figure 7–18 Install Application Assistant - Page 3

Install Application Assistant

Back Next Finish Cancel

Select deployment targets

Select the servers and/or clusters to which you want to deploy this application. (You can reconfigure deployment targets later).

Available targets for jpdk :

Servers
<input type="checkbox"/> AdminServer
<input type="checkbox"/> WC_Portlet
<input type="checkbox"/> WC_Services
<input type="checkbox"/> WC_Spaces
<input type="checkbox"/> WC_CustomPortal

Back Next Finish Cancel

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 24.2.1, "Registering a WSRP Producer Using Fusion Middleware Control"](#) and [Section 24.4.1, "Registering an Oracle PDK-Java Producer Using Fusion Middleware Control"](#)) or WLST commands (see [Section 24.2.2, "Registering a WSRP Producer Using WLST"](#) or [Section 24.4.2, "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 Framework Applications Using Fusion Middleware Control."](#)

7.1.6.7 Saving and Reusing the Deployment Plan

A deployment plan contains the configuration data needed to deploy an archive to a Managed Server. You can create a deployment plan while you're building and testing your application, or when you deploy your EAR file using Fusion Middleware Control as described in [Section 7.1.6.4, "Deploying Applications Using Fusion Middleware Control."](#) If there are deployment descriptors packaged within the EAR file, the deployment uses the data in these files. If you need to make any changes to the `web.xml` file, Oracle recommends that you create a deployment plan.

Once created, a deployment plan can be saved as part of the application properties on the target Managed Server, and re-used when redeploying the application using Fusion Middleware Control, as described in [Section 7.3.2, "Redeploying Framework Applications Using Fusion Middleware Control,"](#) or using WLST as described in [Section 7.3.3, "Redeploying Framework Applications Using WLST."](#)

7.1.7 Migrating Customizations and Data Between Environments

You can export and import customizations made to pages, WebCenter Portal services, and portlets (PDK-Java and WSRP version 2 producers) of a deployed application. For more information, see [Chapter 39.2, "Exporting and Importing Framework Applications for Data Migration."](#)

7.1.8 Configuring Applications to Run in a Distributed Environment

For information about configuring your Framework application to run in a distributed environment, see the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle WebCenter Portal*, and "Configuring High Availability for Oracle ADF and WebCenter Portal Applications" in the *Oracle Fusion Middleware High Availability Guide*.

7.2 Undeploying Framework applications

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

Note: When a Framework application is undeployed, its application credentials and MDS customizations are kept in case the application is 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 before 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:

- [Section 7.2.1, "Undeploying Framework Applications Using Fusion Middleware Control"](#)
- [Section 7.2.2, "Undeploying Framework Applications Using WLST"](#)
- [Section 7.2.3, "Removing an Application's Credential Map"](#)

7.2.1 Undeploying Framework Applications Using Fusion Middleware Control

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

To undeploy a Framework 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 Framework Applications Using WLST

This section describes how to undeploy a Framework application using WLST.

To undeploy a Framework application using WLST:

1. Start the WLST shell.

For information on starting the WLST shell, see [Section 1.13.3, "Oracle WebLogic Scripting Tool \(WLST\)."](#)

2. Connect to the Administration Server of your WebCenter Portal 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 Framework 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 7-19](#)).

Figure 7-19 Credentials Pane



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

7.3 Redeploying Framework applications

This section describes how to redeploy a Framework application using Fusion Middleware Control or from the command line using WLST. When you redeploy a new version of an application, you cannot 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 Framework applications"](#).

Note: Some system .EAR files, such as `wcps-services.ear` and `wsrp-tools-as.ear`, are not versioned and were not intended to be redeployed. Redeploying these files will generate an error.

This section contains the following subsections:

- [Section 7.3.1, "Redeployment Considerations"](#)
- [Section 7.3.2, "Redeploying Framework Applications Using Fusion Middleware Control"](#)
- [Section 7.3.3, "Redeploying Framework 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 during run-time:

- 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.

Note: You must delete runtime customizations (customizations not done through JDeveloper) before redeploying an updated application that has had major changes to artifacts such as pages, connections, or task flows.

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

- [Section 7.3.1.1, "Preserving Application Configuration"](#)
- [Section 7.3.1.2, "Preserving Service and User Customizations"](#)
- [Section 7.3.1.3, "Preserving Resource Customizations"](#)
- [Section 7.3.1.4, "Preserving Portlet Customizations"](#)

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 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 does not display after deployment, and you must re-create it.
- A connection property has been changed in the packaged configuration. The customized properties are 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 WLST commands to configure the Framework application, you can easily combine them into a script to remove all the connections and re-create 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 Service and User Customizations

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

Application and user customizations 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 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 appear as they are.
- If elements are removed from the package, for which customizations were created, those 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 application and user customizations in a production application instance and import it into a test or staging instance. You can then test the application against those customizations to see that the new changes do not have an undesired impact.

7.3.1.3 Preserving Resource Customizations

Users can create new resources at runtime using the Resource Manager. If you plan to redeploy the application and want to preserve runtime-created resources, before redeployment you must first download the resources from the running application and import the resulting archive file into the design-time environment.

If you do not download and import runtime-created resources, they are lost upon redeployment of the application. Any new pages created at runtime that use the lost resources are still available even though the resources themselves are no longer available in the Resource Manager. This is because the

generic-site-resources.xml file, which is updated at runtime when new resources are created, is overwritten on redeployment by the design-time version of the file.

7.3.1.4 Preserving Portlet Customizations

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 before redeployment, then those modified connections are used to identify target producers. Note that if you redeploy an EAR file with the same checksum (that is, the same file) as the pre-existing one, portlet customization and personalizations are not overwritten.

7.3.2 Redeploying Framework Applications Using Fusion Middleware Control

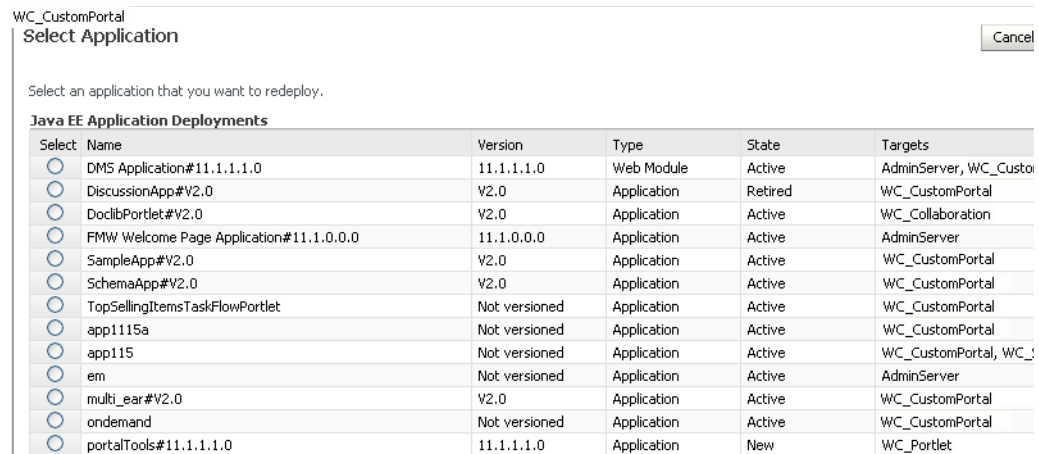
This section describes how to redeploy a Framework application using Fusion Middleware Control.

To redeploy a Framework 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 7-20](#)).

Figure 7-20 Select Application Page



4. Select the application that you want to redeploy.
5. Click **Next** to display the Select Archive page (see [Figure 7-21](#)).

Figure 7–21 Select Archive Page

Select Archive ? Cancel Step 1 of 4 Next

Specify the application or the exploded directory. Optionally you can specify a deployment plan.

Archive or Exploded Directory
 Java EE archive, Web Modules (WAR files), EJB Modules (EJB JAR files) and Resource Adapter Modules (RAR files) can be deployed. You can also deploy an exploded archive that is present on the server where Enterprise Manager is running.

Archive is on the machine where this web browser is running.
 Archive or exploded directory is on the server where Enterprise Manager is running.

Deployment Plan
 The deployment plan is a file that contains the deployment settings for an application. You can use a previously saved deployment plan for this application. Later in the deployment process, you can optionally edit the deployment plan and save it for a future deployment of this application. If you do not have a deployment plan, one will be created automatically during the deployment process when deployment configuration is done.


Create a new deployment plan when deployment configuration is done.
 Deployment plan is on the machine where this web browser is running.
 Deployment plan is on the server where Enterprise Manager is running.

Information
 Use this page to deploy Java EE applications that require Oracle Metadata Services (MDS) or that take advantage of the Oracle Application Development Framework (Oracle ADF).
 If your application is a SOA composite, use the SOA Composite deployment wizard.
 If your application is not a SOA composite or it does not require an MDS repository or ADF connections, then you can deploy your application using this wizard or the Oracle WebLogic Server Administration Console.

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 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 7–22](#)).

Figure 7–22 Application Attributes Page

Application Attributes  Cancel Back Step 3 of 4


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-CustomDS 
 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. If you do not, all customizations are lost.

11. Click Next.




The Deployment Settings page displays (see [Figure 7–23](#)).

Figure 7–23 Deployment Settings Page

Deployment Settings Cancel

Archive Type Java EE Application (EAR file) Application Name ondemand
 Archive Location /net/example/scratch/custom_apps/5341/ondemand.ear Version V2.0
 Deployment Plan Create a new plan Context Root ondemand
 Deployment Target WC_CustomPortal Deployment Mode Distribute and start application (servicing all r

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 <code>connections.xml</code> 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
 - Configure ADF connection settings
13. Click the **edit** icon for Configure ADF Connections to check connection settings associated with the Framework 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 7–24](#)).

Figure 7–24 Configure ADF Connections Page

Configure ADF Connections Cancel Step 1

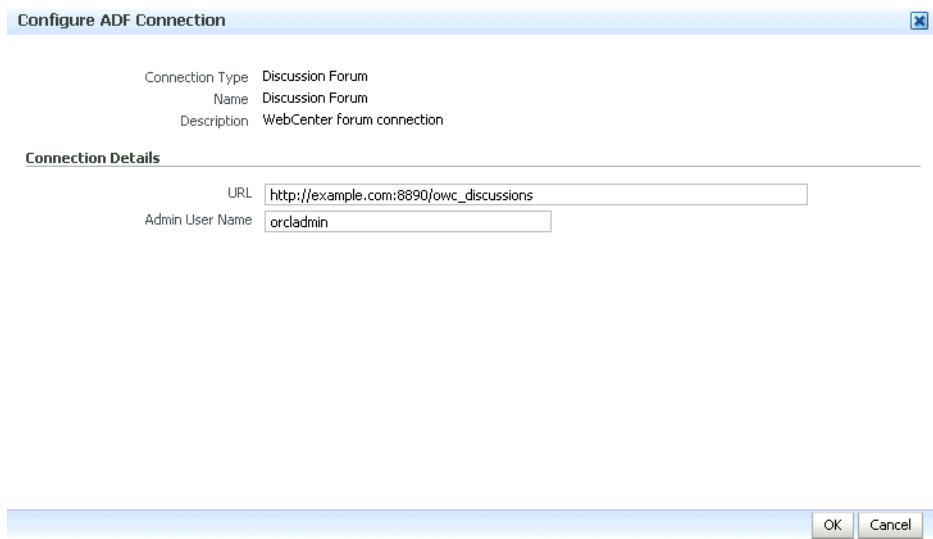
ADF Connections
Configure the ADF connections defined in connections.xml in this application.

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).

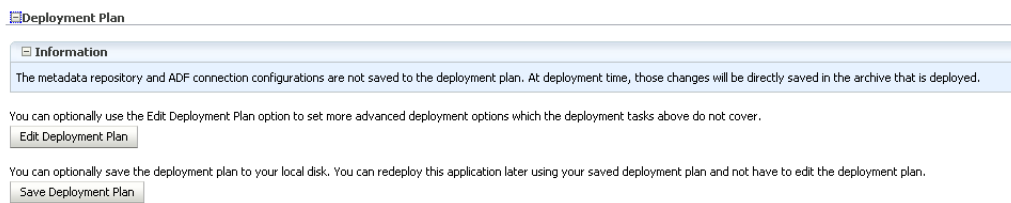
For a Discussion Forum connection (shown in [Figure 7–14](#)), for example, ensure that the URL to the discussions server, and the user account used to connect to the server are correct for the target environment.

Figure 7–25 Discussion Forum Connection Settings



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 7–26](#)).

Figure 7–26 Deployment Settings Page - Deployment Plan Section



You can edit and save the deployment plan to your local hard drive, if you choose, so that you can use those settings to redeploy the application again later. See [Section 7.1.6.7, "Saving and Reusing the Deployment Plan"](#) for more information about deployment plans.

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 Framework Applications Using WLST

To redeploy a Framework 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 Framework application using WLST:

1. Start the WLST shell.

For information on starting the WLST shell, see [Section 1.13.3, "Oracle WebLogic Scripting Tool \(WLST\)."](#)

2. Connect to the administration server of your WebCenter Portal 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.

7.4 Post-Deployment Configuration

After your Framework application is deployed, you must check that the settings that were deployed are valid for the target Managed Server. Settings to check include those for security, connections, and data sources.

This section includes the following subsections:

- [Section 7.4.1, "Checking Security Configurations After Deployment"](#)
- [Section 7.4.2, "Checking Application Connections After Deployment"](#)
- [Section 7.4.3, "Checking Data Source Connections"](#)
- [Section 7.4.4, "Tuning the Application"](#)

7.4.1 Checking Security Configurations After Deployment

Before deploying your application you must set up the Identity Store and the Policy and Credential Store on the target Managed Server. After deployment, check that the

application configurations match those of the target server. You should also check that all other applicable post-deployment security configurations, such as SSL and single sign-on, have been properly configured, as described in [Section 28.2.5, "Post-deployment Security Configuration Tasks."](#)

7.4.2 Checking Application Connections After Deployment

After deploying your Framework application, check that all of the connections used by your application have been properly set. Connections that you may have to configure or reconfigure include connections for:

- BPEL Worklists
- External applications
- Discussions server
- Mail server
- Instant Messaging and Presence (IMP) server
- Search
- WSRP producers
- PDK-Java portlet producers
- Web Services
- content repositories
- personal event server
- analytics collector

7.4.3 Checking Data Source Connections

After deploying your Framework application to a custom Managed Server, check that the data sources that you configured during testing are still valid for the deployed application. For information on how to configure data sources for the Metadata Services (MDS) repository your Framework application, see "Configuring JDBC Data Sources" in *Oracle Fusion Middleware Configuring and Managing JDBC Data Sources for Oracle WebLogic Server*. Note that when setting up the data source, you must provide a password or the connection may not be created when the application is deployed.

7.4.4 Tuning the Application

After your Framework application has been deployed and correctly configured, check the system file limit, data source settings, and JRockit virtual machine (JVM) arguments as described in [Section A.4, "Tuning Oracle WebCenter Portal Performance."](#) Also see the chapter on "Oracle WebCenter Portal Performance Tuning" in the *Oracle Fusion Middleware Performance and Tuning Guide*, and [Section 38, "Monitoring Oracle WebCenter Portal Performance"](#) for information on how to diagnose performance problems.

Starting and Stopping WebCenter Portal Applications

Most WebCenter Portal 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 WebCenter Portal services such as Announcements, Discussions, Documents, Mail, and so on, 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 Portal application and any changes that you make to existing connections take effect immediately too.

This chapter includes the following sections:

- [Section 8.1, "Starting Node Manager"](#)
- [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments"](#)
- [Section 8.3, "Starting and Stopping the Spaces Application"](#)
- [Section 8.4, "Starting and Stopping Framework Applications"](#)

You perform all start and stop operations from the Oracle WebLogic Server Administration Console too. See also "Starting and Stopping Servers" in *Oracle Fusion Middleware Managing Server Startup and Shutdown for Oracle WebLogic Server*.

Note: Node Manager *must* be running before you can start and stop administration servers, managed servers, and WebCenter Portal 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 Portal applications through Fusion Middleware Control or Oracle WebLogic Server Administration Console. Node Manager starts after installation, so you only need to restart Node Manager if someone specifically shuts it down.

For information on how to start Node Manager with `startNodeManager.sh`, see "Using Node Manager" in the *Oracle Fusion Middleware Node Manager Administrator's Guide for Oracle WebLogic Server*.

8.2 Starting and Stopping Managed Servers for WebCenter Portal Application Deployments

Most WebCenter Portal 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.

When you start or restart a managed server, all applications deployed on the managed server start automatically, see also [Table 8-1](#).

Table 8-1 Oracle WebCenter Portal Managed Servers and Applications

Managed Server	Application(s)
WC_Spaces	webcenter (Spaces Application)
	webcenter-help (Spaces Online Help)
WC_Portlet	portalTools (OmniPortlet and Web Clipping)
	wsrp-tools (WSRP Tools)
	pagelet-producer (Pagelet Producer)
	services-producer (WebCenter Services Producer)
WC_Collaboration	owc_discussions (Discussions Server)
WC_Uilities	analytics-collector (Analytics)
	activitygraph-engines (Activity Graph)
	wcps-services (Personalization Services)
WC_CustomPortal	<your_webcenter_portal_framework_application_name>

Note: This section describes how to start and stop WebCenter Portal managed servers listed in [Table 8-1](#). To start and stop managed servers for other components, refer to:

- Oracle WebCenter Content managed server, see *Oracle WebCenter Content Installation Guide*
- Oracle SOA Server managed server, see *Oracle Fusion Middleware Installation Guide for Oracle SOA Suite and Oracle Business Process Management Suite*

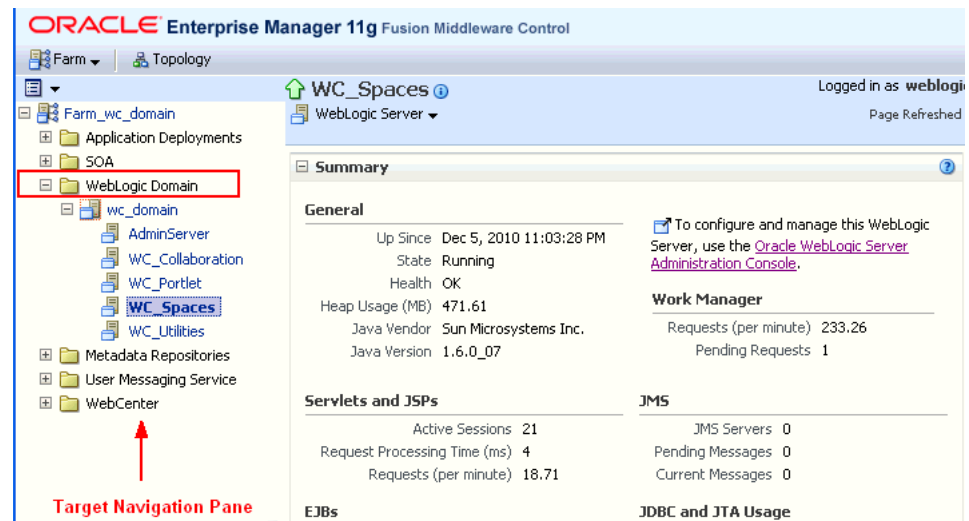
While a specific order in which to start managed servers is not mandated, if you must start multiple managed servers, it is good practice to start the managed server on which Spaces or your Framework application is deployed last.

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

1. Login to Fusion Middleware Control.
2. Expand **WebLogic Domain** in the Target Navigation Pane.
3. Expand **wc_domain**, and select the managed server you want to start or stop.

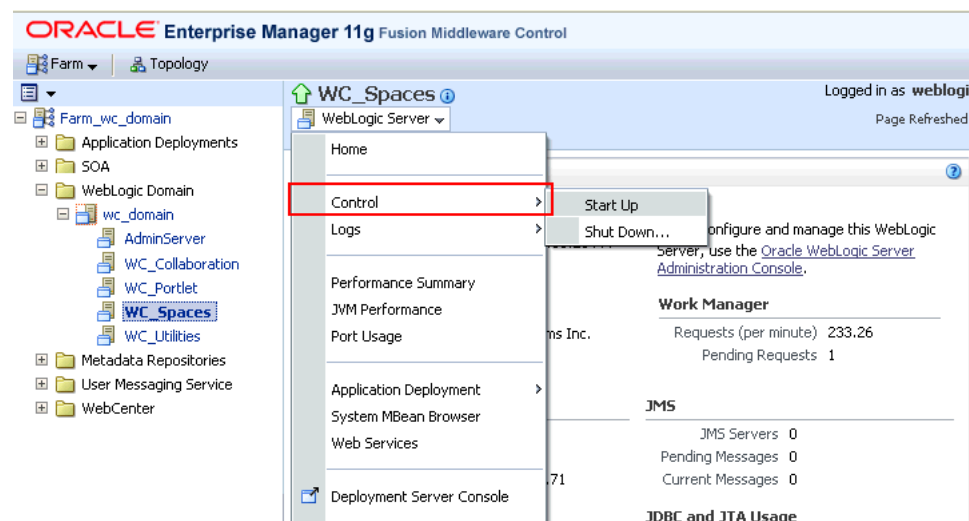
The home page for the managed server displays (Figure 8–2).

Figure 8–1 Managed Server Home Page



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

Figure 8–2 Managed Server Start Up or Shut Down



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

To start and stop WebCenter Portal managed servers using command line tools, see "Starting and Stopping WebLogic Managed Servers Using the Command Line" in *Oracle Fusion Middleware Administrator's Guide*.

8.3 Starting and Stopping the Spaces Application

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

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

Alternatively, use WLST:

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

You can also start Spaces through Oracle WebLogic Server Administration Console.

Note: Application configuration changes require you to restart the *WC_Spaces managed server* on which Spaces is deployed. For details, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments"](#).

8.3.1 Starting Spaces Using Fusion Middleware Control

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

To start Spaces through Fusion Middleware Control:

1. In Fusion Middleware Control, navigate to the home page for the Space application.
See [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#).
2. From the main WebCenter Portal menu, choose **WebCenter > Portal > Control > Start Up**.

Alternatively, right-click **WC_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 Spaces Using WLST

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

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

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

8.3.3 Stopping Spaces Using Fusion Middleware Control

When you stop the Spaces application 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 Spaces, the managed server on which the Spaces application is deployed (WC_Spaces) remains available.

To stop a Spaces application through Fusion Middleware Control:

1. In Fusion Middleware Control, navigate to the home page for Spaces.
See [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#).
2. From the main menu, choose **WebCenter > Portal > Control > Shut Down**.
Alternatively, right-click **WC_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 Spaces Using WLST

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

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

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

8.4 Starting and Stopping Framework Applications

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

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

Alternatively, use WLST:

- [Starting Framework Applications Using WLST](#)
- [Stopping Framework Applications Using WLST](#)

You can also start Framework applications through Oracle WebLogic Server Administration Console.

Note: Application configuration changes require you to restart the *managed server* on which the Framework application is deployed. For details, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments"](#).

8.4.1 Starting Framework Applications Using Fusion Middleware Control

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

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

To start a Framework application through Fusion Middleware Control:

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

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

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

Alternatively, right-click the name of the Framework 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 Framework Applications Using WLST

Use the WLST command `startApplication` to start a Framework 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 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

8.4.3 Stopping Framework Applications Using Fusion Middleware Control

When you stop a Framework application 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 Portal: Spaces through Oracle WebLogic Server Administration Console.

To stop a Framework application:

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

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

2. From the main menu, choose **Application Deployment >Control > Shut Down**.

Alternatively, right-click the name of the Framework 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 Framework Applications Using WLST

Use the WLST command `stopApplication` to stop a Framework 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 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

Setting WebCenter Portal Application Properties

This chapter includes the following sections:

- [Section 9.1, "Setting Application Properties for the Spaces Application"](#)
- [Section 9.2, "Setting Application Properties for Framework Applications"](#)
- [Section 9.3, "Specifying the BPEL Server Hosting Spaces Workflows"](#)
- [Section 9.4, "Configuring Search Crawlers"](#)
- [Section 9.5, "Setting Search Options"](#)
- [Section 9.6, "Choosing a Channel for Notification Messages"](#)
- [Section 9.7, "Setting Up a Proxy Server"](#)
- [Section 9.8, "Exposing Spaces Templates From a Previous Release"](#)
- [Section 9.9, "Setting a Session Timeout for the Spaces Application"](#)

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 the Spaces Application

The Spaces home page (in Fusion Middleware Control) is your starting place for configuring Spaces application deployments. Just like any other J2EE application, you can configure ADF, MDS, security policies and roles, and so on, from here. You can also configure back-end service connections, external applications, and portlet producers for the Spaces application. To access this page, see [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#).

Additionally, there are several application-level settings for configuring Spaces workflows and Oracle SES search crawling in Spaces. Application settings are described in the following sections:

- [Section 9.3, "Specifying the BPEL Server Hosting Spaces Workflows"](#)
- [Section 9.4, "Configuring Search Crawlers"](#)
- [Section 9.5, "Setting Search Options"](#)
- [Section 9.6, "Choosing a Channel for Notification Messages"](#)

- [Section 9.7, "Setting Up a Proxy Server"](#)
- [Section 9.8, "Exposing Spaces Templates From a Previous Release"](#)
- [Section 9.9, "Setting a Session Timeout for the Spaces Application"](#)

9.2 Setting Application Properties for Framework Applications

The J2EE Application Deployment home page (in Fusion Middleware Control) is your starting place for configuring application deployments developed with WebCenter Portal: Framework. Just like any other J2EE application, you can configure ADF, MDS, security policies and roles, and so on, from here. You can also configure back-end service connections, external applications, and portlet producers. To access this page, see [Section 6.3, "Navigating to the Home Page for Framework Applications"](#).

Additionally, there are several application-level settings for configuring proxy servers, search settings, and a notification channel for the Framework application. Application settings are described in the following sections:

- [Section 9.4, "Configuring Search Crawlers"](#)
- [Section 9.5, "Setting Search Options"](#)
- [Section 9.6, "Choosing a Channel for Notification Messages"](#)
- [Section 9.7, "Setting Up a Proxy Server"](#)

See also, [Appendix A.4, "Tuning Oracle WebCenter Portal Performance"](#).

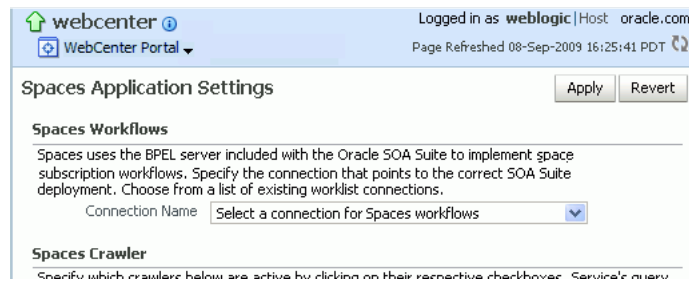
9.3 Specifying the BPEL Server Hosting Spaces Workflows

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

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

To configure a connection to Spaces workflows:

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

Figure 9–1 Choosing the BPEL Server Where Spaces Workflows are Deployed

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

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

Ensure that you choose the connection that points to the SOA instance in which Spaces workflows are deployed. If that connection is not listed you must create it. To define the connection, see [Section 23.4, "Setting Up Worklist Connections"](#).

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

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

9.4 Configuring Search Crawlers

Post deployment, administrators can configure search crawlers for Spaces or their Framework application. Both Spaces and Framework applications can use either Oracle Secure Enterprise Search (SES) or WebCenter Portal's own search adapters. Search crawler configuration for the Spaces application is slightly different to other Framework applications, so ensure that you follow the appropriate documentation for your application.

Spaces Application

Out-of-the-box, the Spaces application uses WebCenter Portal's own Search service for searching and returning Spaces content. If preferred, you can use Oracle Secure Enterprise Search (SES) to search and return unified results for most Spaces resources, including documents, discussions, announcements, spaces, lists, pages, wikis and blogs. To set up Oracle SES searching, see [Section 22.6, "Configuring Oracle SES to Search Spaces Applications"](#).

Framework Applications

By default, Framework applications are configured to use Oracle SES crawlers. If you do not want to use Oracle SES you can specify that WebCenter Portal's own search adapters are used instead. For details, see [Section 22.5, "Configuring Oracle SES to Search Framework Applications"](#).

9.5 Setting Search Options

Post deployment, administrators can fine-tune search settings to suit their WebCenter Portal application. For example, you can set suitable search timeouts and specify how many search results to return and display.

Note: The following steps describe how to set search options using Fusion Middleware Control. You can set the same options using WLST commands, for details, see "setSearchConfig" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

To set search parameters using Fusion Middleware Control:

1. Login to Fusion Middleware Control, and navigate to the home page for your WebCenter Portal application:
[Section 6.2, "Navigating to the Home Page for the Spaces Application"](#).
[Section 6.3, "Navigating to the Home Page for Framework Applications"](#).
2. From the **WebCenter Portal** menu, choose **Settings > Application Configuration**.
3. Configure **Search Settings** as required.

Element	Description
Oracle Secure Enterprise Search Data Group	Specify the Oracle SES data group in which to search. If no value is provided, then everything in the Oracle SES instance is searched.
Execution Timeout (ms)	Enter the maximum time that a service is allowed to execute a search (in ms).
Executor Preparation Timeout (ms)	Enter the maximum time that a service is allowed to initialize a search (in ms).
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. Users can click Show All if they want to see all the results.
Number of Saved Searches in Search Page	Enter the number of saved searches displayed in the Saved Search list (on the main search page).

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

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

9.6 Choosing a Channel for Notification Messages

In Spaces and Framework applications, users can subscribe to services and application objects in which they have a particular interest and are subsequently notified of changes and updates that affect their subscribed services and objects.

Notification messages can be routed through a BPEL server or a mail server and it is the system administrator's job to configure the channel that is used. For more information, see [Section 19.2, "Setting Up Notifications"](#).

9.7 Setting Up a Proxy Server

A proxy server is required if you want to enable external RSS news feeds and external links in Activity Stream task flows in your WebCenter Portal application. The RSS service and the Activity Stream service share the same proxy server settings.

You can set up a proxy server using Fusion Middleware Control or WLST.

This section includes the following subsections:

- [Section 9.7.1, "Setting Up a Proxy Server Using Fusion Middleware Control"](#)
- [Section 9.7.2, "Setting Up a Proxy Server Using WLST"](#)

9.7.1 Setting Up a Proxy Server Using Fusion Middleware Control

To set up a proxy server using Fusion Middleware Control:

1. Log on to Fusion Middleware Control and navigate to the home page for your WebCenter Portal application:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **Settings > Application Configuration**.
 - For a Framework application - From the **Application Deployment** menu, choose **WebCenter Portal > Application Configuration**.
3. In the **Proxy Server** section, enter the host name and the port number of the proxy server. For details, see [Table 9-1](#).

Table 9-1 *RSS Proxy Server Details*

Field	Description
Proxy Host	Enter the host name of the proxy server.
Proxy Port	Enter the port number on which the proxy server is running.

4. Click **Apply** to save this connection.
5. Restart the managed server to which your WebCenter Portal application is deployed. For more information, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

9.7.2 Setting Up a Proxy Server Using WLST

Use the WLST command `setRssProxyConfig` to specify the proxy host and port number used by RSS news feeds and Activity Stream task flows. For command syntax and examples, see the section, "setRssProxyConfig" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information about how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

Note: To start using the new proxy details, you must restart the managed server in which your WebCenter Portal application is deployed. For more information, see the section, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in *Oracle Fusion Middleware Administrator's Guide*.

Use the `getRssProxyConfig` command to find out the current proxy host and port used by RSS and Activity Stream task flows. If you want to delete the current proxy host and port settings, use the `unsetRssProxyConfig` command. For more information, see the section "RSS News Feeds" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

9.8 Exposing Spaces Templates From a Previous Release

Out-of-the-box, the Spaces application provides several templates for building spaces, including *Team Site*, *Portal Site*, *Document Exchange*, and more. For details, see "Working with Space Templates" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

Previous releases of Spaces supplied a different template set, namely *Basic*, *Community Of Interest*, and *Group Project*. While Oracle considers these templates deprecated, you can expose them in your latest Spaces version as follows:

1. Log in to SQLPlus as DBA or another administrative user to the WebCenter Portal database.
2. Execute one or more of the following commands:

- **To expose the Basic template:**

```
insert into WC_SPACE_HEADER values

('webcenter',
'sdfcd3cd3_8a53_4a7c_872f_74de46969cef','Basic','Basic','Template for a
Space with minimal initial content',

'Y','N','N','N','N','N','N','N',1,'/oracle/webcenter/space/metadata/spacete
mplate/Basic/images/wc_blank_icon.png',

'/oracle/webcenter/space/metadata/spacetemplate/Basic/images/wc_blank_logo.
png','Blank','system','30-OCT-09 12.00.00.000000000 AM',

'weblogic','30-OCT-09 12.00.00.000000000 AM','','','Y',0,0,1);
```

- **To expose the Community of Interest template:**

```
insert into WC_SPACE_HEADER values

('webcenter', 's5dd6d6b3_7f5f_4f1c_8ee6_ce305469f1b3', 'ProjectSpace', 'Group
Project', 'Template for a Space based on completing a project',

'Y','N','N','N','N','N','N','N',1,'/oracle/webcenter/space/metadata/spacete
mplate/ProjectSpace/images/wc_prj_icon.png',

'/oracle/webcenter/space/metadata/spacetemplate/ProjectSpace/images/wc_prj_
logo.png','project,group,team','system','30-OCT-09 12.00.00.000000000 AM',

'weblogic','30-OCT-09 12.00.00.000000000 AM','','','Y',0,0,1);
```


- **To expose the Group Project template:**

```
insert into WC_SPACE_HEADER values

('webcenter',
'sb175bdde_4cb8_4da8_bcdb_eff13e59da2d', 'CommunityOfInterest', 'Community of
Interest', 'Template for a Space based on a common interest',

'Y', 'N', 'N', 'N', 'N', 'N', 'N', 'N', '1', '/oracle/webcenter/space/metadata/spacete
mplate/CommunityOfinterest/images/coi_icon.png',

'/oracle/webcenter/space/metadata/spacetemplate/CommunityOfinterest/images/
coi_logo.png', 'community', 'system', '30-OCT-09 12.00.00.000000000 AM',

'weblogic', '30-OCT-09 12.00.00.000000000 AM', '', '', '', 'Y', 0, 0, 1);
```

The templates are available immediately. You are not required to restart the Spaces application.

9.9 Setting a Session Timeout for the Spaces Application

A default session timeout for a Spaces application is derived from the HTTP session timeout specified in `web.xml`. Out-of-the-box, the `web.xml` setting for `<session-timeout>` is 45 minutes.

Administrators can use the `wcSessionTimeoutPeriod` attribute in `webcenter-config.xml` to increase or decrease the session timeout if required.

To modify the session timeout for the Spaces application:

1. Export the latest `webcenter-config.xml` from MDS.

For example:

```
exportMetadata(application='webcenter', server='WC_Spaces',
toLocation='/tmp/mydata',
docs='/oracle/webcenter/webcenterapp/metadata/mdssys/cust/site/webcenter/webcen
ter-config.xml.xml')
```

The `webcenter-config.xml` file is created the first time you configure "General" settings through Spaces administration. See also, [Appendix A.1.3, "webcenter-config.xml"](#).

Note: `webcenter-config.xml` is created in MDS the first time you configure "General" settings through Spaces Administration. If the file does not yet exist in MDS you can edit `webcenter-config.xml` directly. The file is located at:
`/oracle/webcenter/webcenterapp/metadata/webcenter-co
nfig.xml`

2. Open `webcenter-config.xml.xml` exported from MDS in a text editor and add the following snippet:

```
<mds:replace
node="wcSessionTimeoutPeriod(xmlns(mds_nsl=http://xmlns.oracle.com/webcenter/we
bcenterapp))/mds_nsl:value"/>
<mds:insert
after="wcSessionTimeoutPeriod(xmlns(mds_nsl=http://xmlns.oracle.com/webcenter/w
ebcenterapp))/mds_nsl:type" parent="wcSessionTimeoutPeriod">
```

```
<value xmlns="http://xmlns.oracle.com/webcenter/webcenterapp">15</value>
</mds:insert>
```

3. For *value*, enter the timeout you require (in minutes).
4. Save and close `webcenter-config.xml.xml`.
5. Import the updated `webcenter-config.xml.xml` file to MDSs.

For example:

```
importMetadata(application='webcenter', server='WC_Spaces',
fromLocation='/tmp/mydata',
docs='/oracle/webcenter/webcenterapp/metadata/mdssys/cust/site/webcenter/webcen
ter-config.xml.xml')
```

Part IV

Managing Services, Portlet Producers, and External Applications

The chapters in this part present administration tasks for Oracle WebCenter Portal's services, portlet producers, and external applications.

Part IV contains the following chapters:

- Chapter 10, "Managing Oracle WebCenter Portal Services"
- Chapter 11, "Managing Content Repositories"
- Chapter 12, "Managing the Activity Graph Service"
- Chapter 13, "Managing the Analytics Service"
- Chapter 14, "Managing the Announcements and Discussions Services"
- Chapter 15, "Managing the Events Service"
- Chapter 16, "Managing the Instant Messaging and Presence Service"
- Chapter 17, "Managing the Mail Service"
- Chapter 19, "Managing Subscriptions and Notifications"
- Chapter 20, "Managing Personalization for WebCenter Portal"
- Chapter 21, "Managing the RSS Service"
- Chapter 22, "Managing Oracle SES Search in WebCenter Portal"
- Chapter 23, "Managing the Worklist Service"
- Chapter 24, "Managing Portlet Producers"
- Chapter 25, "Managing Oracle WebCenter Portal's Pagelet Producer"
- Chapter 26, "Managing External Applications"
- Chapter 27, "Managing REST Services"

Managing Oracle WebCenter Portal Services

This chapter provides an overview of managing services in WebCenter Portal applications. It also explains the back-end repositories required for the various services.

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). For more information, see [Section 1.8, "Understanding Administrative Operations, Roles, and Tools."](#)

10.1 Introduction to Managing Services

WebCenter Portal exposes collaborative, social networking, and personal productivity features through *services*, which, in turn, expose subsets of their features and functionality through *task flows*. Task flows provide reusable functionality that may expose all or a subset of the features available from a particular service.

Always use Fusion Middleware Control or the WLST command-line tool to review and configure back-end services for WebCenter Portal applications.

Note: Most changes that you make to services configuration, through Fusion Middleware Control or using WLST, are not dynamic so you must restart the managed server on which the WebCenter Portal application is deployed for your changes to take effect. For more information, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

[Table 10–1](#) lists where data for services is stored. It may be helpful to know what services are impacted when repositories are unavailable.

- Some services store connection metadata in the Metadata Services Repository (MDS). Changes that you make to applications, post deployment, are stored in MDS as customizations. For more information, see [Section 1.3.5, "WebCenter Portal Configuration Considerations."](#) For more information, see [Section 10.1.1, "Setting Up the MDS Repository."](#)
- Some services require a connection to a database schema where relevant information (such as relationship mapping) is stored. For more information, see [Section 10.1.2, "Setting Up Database Connections."](#)
- Some services require a connection to an external data repository (such as a content server, a presence server, or a mail server) where relevant information is

stored. For more information on setting up those connections, see the chapter for that service.

Table 10–1 Services Data Repositories

WebCenter Portal Service	Description	MDS	Database Schema	External Repository	For More Information
Activity Graph	Leverages collective intelligence to benefit search and social applications		ACTIVITIES schema		Section 10.1.2, "Setting Up Database Connections"
Analytics	Enables you to display usage and performance metrics for your portal application		ACTIVITIES schema	X	Section 10.1.2, "Setting Up Database Connections" Chapter 13, "Managing the Analytics Service"
Announcements	Provides the ability to post announcements about important activities and events to all authenticated users	X		X	Section 10.1.1, "Setting Up the MDS Repository" Chapter 14, "Managing the Announcements and Discussions Services"
Discussions	Provides the ability to create threaded discussions, posing and responding to questions and searching for answers	X		X	Section 10.1.1, "Setting Up the MDS Repository" Chapter 14, "Managing the Announcements and Discussions Services"
Documents	Provides content management and storage capabilities, including content upload, file and folder creation and management, file check out, versioning, and so on	X	WEBCENTER schema - for documents (including wikis and blogs) that want to include comments and Activity Stream	X	Section 10.1.1, "Setting Up the MDS Repository" Section 10.1.2, "Setting Up Database Connections" Chapter 11, "Managing Content Repositories"
Events	Provides the ability to create and maintain a schedule of events relevant to a wider group of authenticated users	X		X (Personal Events)	Section 10.1.1, "Setting Up the MDS Repository" Chapter 15, "Managing the Events Service"
Instant Messaging and Presence (IMP)	Provides the ability to observe the status of other authenticated users (online, offline, busy, or away) and to contact them instantly			X	Chapter 16, "Managing the Instant Messaging and Presence Service"
Links	Provides the ability to view, access, and associate related information; for example, you can link to a document from a discussion		WEBCENTER schema		Section 10.1.2, "Setting Up Database Connections"

Table 10–1 (Cont.) Services Data Repositories

WebCenter Portal Service	Description	MDS	Database Schema	External Repository	For More Information
Lists	Provides the ability to create, publish, and manage lists	X	WEBCENTER schema		Section 10.1.1, "Setting Up the MDS Repository" Section 10.1.2, "Setting Up Database Connections"
Mail	Provides easy integration with IMAP and SMTP mail servers to enable users to perform mail functions, such as reading messages, creating messages with attachments, replying to or forwarding messages, and deleting messages	X		X	Section 10.1.1, "Setting Up the MDS Repository" Chapter 17, "Managing the Mail Service"
Notes	Provides the ability to "jot down" and retain bits of personally relevant information Note: This service is available only in Oracle WebCenter Portal: Spaces.	X			Section 10.1.1, "Setting Up the MDS Repository"
Notifications	Provides a means of subscribing to services and application objects and, when those objects change, receiving notification across one or more messaging channels				Chapter 19, "Managing Subscriptions and Notifications"
People Connections	Provides social networking capabilities, such as creating a personal profile, displaying current status, and viewing other users' recent activities		WEBCENTER schema		Section 10.1.2, "Setting Up Database Connections"
Personalization	Enables you to deliver content within your application to targeted application users based on selected criteria				Chapter 20, "Managing Personalization for WebCenter Portal"
Polls	Enables you to survey your audience (such as their opinions and their experience level), check whether they can recall important information, and gather feedback		WEBCENTER schema		Section 10.1.2, "Setting Up Database Connections"
Recent Activities	Provides a summary view of recent changes to documents, discussions, and announcements	X			Section 10.1.1, "Setting Up the MDS Repository"

Table 10–1 (Cont.) Services Data Repositories

WebCenter Portal Service	Description	MDS	Database Schema	External Repository	For More Information
RSS	Provides the ability to access the content of many different web sites from a single location—a news reader	X			Section 10.1.1, "Setting Up the MDS Repository"
Search	Provides the ability to search services, the application, or an entire site (This includes integrating Oracle Secure Enterprise Search.)	X		X	Section 10.1.1, "Setting Up the MDS Repository" Chapter 22, "Managing Oracle SES Search in WebCenter Portal"
Tags	Provides the ability to assign one or more personally-relevant keywords to a given page or document	X	WEBCENTER schema		Section 10.1.1, "Setting Up the MDS Repository" Section 10.1.2, "Setting Up Database Connections"
Worklists	Provides a personal view of business processes that require attention	X		X	Section 10.1.1, "Setting Up the MDS Repository" Chapter 23, "Managing the Worklist Service"

10.1.1 Setting Up the MDS Repository

Some services store information in the Metadata Services Repository (MDS). To enable these services in WebCenter Portal applications, you must configure the MDS repository. For information, see [Section 7.1.5, "Creating and Registering the Metadata Service Repository."](#)

See Also: "Managing the Oracle Metadata Repository" and "Purging Oracle WebCenter Portal Data" in the *Oracle Fusion Middleware Administrator's Guide*

10.1.2 Setting Up Database Connections

Many services store information in the WebCenter Portal repository, which is a database with the WebCenter Portal schema (WEBCENTER) installed. For example, with the Links service, relationship mapping information, such as what object is linked to what other object, is stored in the database. The WebCenter Portal schema is included with the product.

For WebCenter Portal: Framework applications, you must set up a database connection to the WebCenter Portal repository. This database connection can be of type **JDBC Data Source** or **JDBC URL**.

Note: For WebCenter Portal: Spaces, a WebCenter Portal repository is configured out-of-the-box, and repository connection does not require reconfiguration.

See Also:

- "Setting Up a Database Connection" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal* for information on creating the connection and installing the schema
- [Section 7.1.6, "Deploying the Application to a WebLogic Managed Server"](#) for data source considerations when deploying your application to a production environment
- [Chapter 39, "Managing Export, Import, Backup, and Recovery of WebCenter Portal"](#) for information on backing up and migrating this information

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 Data Sources 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 has 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 Data Sources 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 the *Oracle Fusion Middleware Application 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 WebCenter Portal: Framework applications from development to production, you must 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 the 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`, then the JNDI name is `jdbc/connection1DS`.

10.1.3 Setting Up External Application Connections

When a service interacts with an application that handles its own authentication, you can associate that application with an external application definition to allow for credential provisioning.

The following services permit the use of an external application to connect with the service and define authentication for it:

- Documents

- Events
- Instant Messaging and Presence
- Mail
- RSS Viewer (when using a secured RSS feed)

See Also: [Chapter 26, "Managing External Applications"](#)

Managing Content Repositories

This chapter describes how to configure and manage content repositories used by WebCenter Portal applications.

This chapter contains the following sections:

- [Section 11.1, "What You Should Know About Content Repositories"](#)
- [Section 11.2, "Configuring Oracle WebCenter Content Server Repositories"](#)
- [Section 11.3, "Configuring Microsoft SharePoint Repositories"](#)
- [Section 11.4, "Configuring Oracle Portal Repositories"](#)
- [Section 11.5, "Configuring a File System Repository"](#)
- [Section 11.6, "Registering Content Repositories"](#)
- [Section 11.7, "Changing the Active \(or Default\) Content Repository Connection"](#)
- [Section 11.8, "Modifying Content Repository Connection Details"](#)
- [Section 11.9, "Deleting Content Repository Connections"](#)
- [Section 11.10, "Setting Connection Properties for the Spaces Content Repository"](#)
- [Section 11.11, "Testing Content Repository Connections"](#)
- [Section 11.12, "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 [Section 1.8, "Understanding Administrative Operations, Roles, and Tools"](#).

11.1 What You Should Know About Content Repositories

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

Oracle WebCenter Portal 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 a WebCenter Portal: Framework application.

- The Documents service, which enables users to view and manage documents and other types of content in your organization's content repositories.
- Content Presenter, which enables end users to select content in a variety of ways and then display those items using available display templates. A Content Presenter task flow can be added during development of a WebCenter Portal: Framework application, or can be added to editable pages at runtime.

For more information about managing and including content in WebCenter Portal applications, see also:

- "Integrating Content" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal* to configure content repository connections that provide access to decentralized content.
- "Creating Custom Content Presenter Display Templates" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal* to create custom display templates to integrate and publish decentralized content in your WebCenter Portal application using Content Presenter.
- "Configuring Content Repository Connections" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal* to use Java Content Repository (JCR) controls to enable read-only access to a content repository.
- "Integrating the Documents Service" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal* to integrate the Documents service in WebCenter Portal: Framework applications to provide end users with a user-friendly interface to manage, display, and search documents at runtime.
- "Working with the Documents Service" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces* to work with the Documents service and task flows at runtime in WebCenter Portal applications.

Note: 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 Portal: Framework application is deployed for your changes to take effect. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments"](#).

Prerequisites for each content repository are described in the following sections:

- [Section 11.2, "Configuring Oracle WebCenter Content Server Repositories"](#)
- [Section 11.3, "Configuring Microsoft SharePoint Repositories"](#)
- [Section 11.4, "Configuring Oracle Portal Repositories"](#)
- [Section 11.5, "Configuring a File System Repository"](#)

WebCenter Portal users need to store, publish, and share files. The Documents service provides content management and storage capabilities for WebCenter Portal 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 Portal applications can support multiple content repository connections) to be made active (default):

- **WebCenter Portal: Spaces** - In the Spaces application, every Home space and any spaces that have the Documents service provisioned have their own document folder. This data is stored in the Oracle WebCenter Content Server (Content

Server) repository, which must be configured as the primary content repository for Spaces. Although Spaces requires that Content Server be the active or default content repository, you can also connect Spaces to any of the other supported repositories. See [Section 11.8, "Modifying Content Repository Connection Details"](#) for information about setting the default content repository, and setting additional Document Spaces properties required for a Spaces content repository.

- **Other WebCenter Portal: Framework applications** - When a content repository is made active (see [Section 11.8, "Modifying Content Repository Connection Details"](#)), the 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 Content Server is the primary active content repository (required for Spaces), the Documents service and Content Server must be connected to the same identity store that is used by that WebCenter Portal application.

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 1.3.5, "WebCenter Portal Configuration Considerations."](#)

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

Once connection details are defined, WebCenter Portal application 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 (Document Manager, Folder 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 Portal: Spaces*.

11.2 Configuring Oracle WebCenter Content Server Repositories

This section provides step-by-step instructions for configuring an Oracle WebCenter Content Server 11g (Content Server) content repository for WebCenter Portal: Spaces and WebCenter Portal: Framework applications. Unless otherwise noted, these instructions are common to both Spaces and Framework applications.

This section contains the following subsections:

- [Section 11.2.1, "Prerequisites to Configuring Content Server"](#)
- [Section 11.2.2, "Configuration Roadmap for Content Server"](#)
- [Section 11.2.3, "Configuring Content Server for WebCenter Portal Applications"](#)

11.2.1 Prerequisites to Configuring Content Server

Read this section to understand the prerequisites and other considerations before continuing with [Section 11.2.3, "Configuring Content Server for WebCenter Portal Applications."](#)

This section includes the following subsections:

- [Section 11.2.1.1, "Installation Prerequisites"](#)

- [Section 11.2.1.2, "Configuration Prerequisites"](#)
- [Section 11.2.1.3, "Security Prerequisites"](#)

11.2.1.1 Installation Prerequisites

Content Server

Prior to configuring Oracle WebCenter Content Server 11g (Content Server), you should already have installed Content Server. Content Server is installed as a part of Oracle WebCenter Content, which is an Oracle Fusion Middleware component, and is described in the Oracle WebCenter Content Installation Guide.

If you already have an earlier version of Content Server installed, upgrade your installation to Oracle WebCenter Content Server 11g prior to configuring Content Server 11g. For information about upgrading to Oracle WebCenter Content Server 11g, see "Upgrading Your Oracle Enterprise Content Management Suite Environment" in the Oracle Fusion Middleware Upgrade Guide for Enterprise Content Management.

Inbound Refinery

Oracle recommends that you also install Oracle WebCenter Content: Inbound Refinery (Inbound Refinery) as part of the installation. Inbound Refinery is a conversion server that manages file conversions for electronic assets such as documents, digital images, and motion videos. It also provides thumbnail functionality for documents and images and storyboarding for videos. You can use Inbound Refinery to convert content items stored in Content Server. Installing Inbound Refinery is also described in the *Oracle WebCenter Content Installation Guide*.

Note: Content Server and Inbound Refinery must be installed in the same domain. Oracle recommends that you install Content Server and Inbound Refinery in the same domain as WebCenter Portal. When they are installed in the same domain, no additional configuration is required to use an external LDAP authentication provider.

11.2.1.2 Configuration Prerequisites

After installing Content Server and Inbound Refinery, you should also have configured the initial post-installation settings described in "Configuring the Content Server Instance" in the *Oracle WebCenter Content Installation Guide*. Settings should be configured for both Content Server and Inbound Refinery including the additional WebCenter Portal-specific instructions provided in the tables below. Be sure to restart the servers after updating the settings.

Content Server

Setting	Description
Server Socket Port	This is the intradoc port that we connect to using RIDC. This value is stored in the configuration file for the Managed Server as <code>IntradocServerPort</code> .
Incoming Socket Connection Address Security Filter	Server filter specifying what machines can access Content Server through a socket connection. This value is stored in the configuration file for the Managed Server as <code>SocketHostAddressSecurityFilter</code> .

Setting	Description
Full Text Search (Optional but recommended)	Internal

Inbound Refinery

Setting	Description
Server Socket Port	This is the intradoc port that we connect to using RIDC. This value is stored in the configuration file for the Managed Server as <code>IntradocServerPort</code> .
Incoming Socket Connection Address Security Filter	Server filter specifying what machines can access Inbound refinery through RIDC. This value is stored in the configuration file for the Managed Server as <code>SocketHostAddressSecurityFilter</code> .
Full Text Search (Optional but recommended)	Internal

11.2.1.3 Security Prerequisites

Content Server must be configured to use the same identity store LDAP server as the Spaces application or Framework application. For information on how to reassociate the identity store with an external LDAP server, see [Section 29.1, "Reassociating the Identity Store with an External LDAP Server."](#)

Content Server and Inbound Refinery must be installed in the same domain. Oracle recommends that you install Content Server and Inbound Refinery in the same domain as WebCenter Portal. When they are installed in the same domain, no additional configuration is required to use an external LDAP authentication provider.

11.2.2 Configuration Roadmap for Content Server

The flow chart in [Figure 11-1](#) provides an overview of the prerequisites and tasks required to get Content Server working in WebCenter Portal applications (Spaces and Framework applications). The steps in the flow chart is described in [Table 11-1](#) and the subsections in [Section 11.2.3, "Configuring Content Server for WebCenter Portal Applications."](#)

Figure 11–1 Configuring Content Server for WebCenter Portal Applications

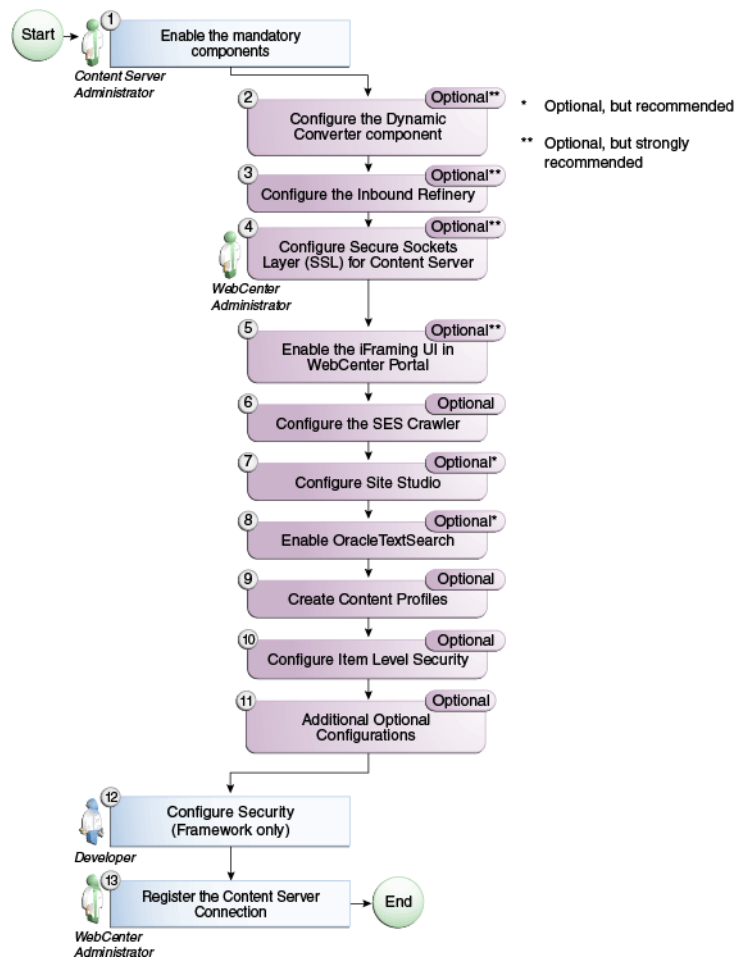


Table 11–1 WebCenter Portal-specific Configuration Tasks for Content Server

Task	Description	Documentation
Enable the mandatory components	Mandatory You must enable the Folders_g component (which provides a hierarchical folder interface to content in Content Server), and the WebCenterConfigure component (which configures an instance of Content Server for WebCenter Portal applications). You must also disable the FrameworkFolders folders component (which is not compatible with the Folders_g component)	See Section 11.2.3.1, "Enabling Mandatory Components."
Configure the Dynamic Converter component	Optional, but strongly recommended This component enables HTML renditions. Slide Previewer is available in WebCenter Portal when both DynamicConverter and the WebCenterConfigure components are installed.	See Section 11.2.3.2, "Configuring the Dynamic Converter Component."

Table 11–1 (Cont.) WebCenter Portal-specific Configuration Tasks for Content Server

Task	Description	Documentation
Configure the Inbound Refinery	<p>Optional, but strongly recommended</p> <p>This is a conversion server that manages file conversions for electronic assets such as documents, digital images, and motion videos. It also provides thumbnail functionality for documents and images and storyboarding for videos. You can use Inbound refinery to convert content items stored in Content Server.</p>	See Section 11.2.3.3, "Configuring the Inbound Refinery."
Configure Secure Sockets Layer (SSL) for Content Server	<p>Optional, but strongly recommended</p> <p>To ensure secure identity propagation, you should set up SSL for Content Server.</p>	See Section 33.7, "Securing the Spaces Connection to Content Server with SSL." Also see Section 11.2.3.4, "Setting Up SSL for Content Server."
Enable the iFraming UI in WebCenter Portal	<p>Optional, but strongly recommended</p> <p>If iFraming is not configured, some functionality, such as Document Manager document rendition support, advanced metadata edit, the IFRAME functionality, and so on, will not be available.</p>	See Section 11.2.3.5, "Enabling the iFraming UI in WebCenter Portal." For more information, also see Appendix B, "Oracle HTTP Server Configuration for WebCenter Portal."
Configure the SES Crawler	<p>Optional</p> <p>You can override the default search adapters and use Oracle SES to get unified ranking results for WebCenter Portal resources such as documents, pages, people, and so on.</p>	See Section 22.6.2, "Setting Up Oracle WebCenter Portal: Content Server for Oracle SES Search." Also see Section 11.2.3.6, "Configuring the SES Crawler."
Configure Site Studio	<p>Optional, but recommended</p> <p>Configuring Site Studio lets you use Site Studio to create and use Site Studio assets (region definitions and display templates) in Content Presenter.</p>	See Section 11.2.3.7, "Setting Up Site Studio." For information, see also the section "Enabling and Disabling a Component" in <i>Oracle WebCenter Content System Administrator's Guide for Content Server</i> and the section "Publishing Content in Content Presenter" in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces</i> . See also <i>Oracle WebCenter Administrator and Manager's Guide for Site Studio</i> .

Table 11–1 (Cont.) WebCenter Portal-specific Configuration Tasks for Content Server

Task	Description	Documentation
Enable OracleTextSearch	<p>Optional, but recommended</p> <p>Although configuring full-text searching and indexing capabilities is optional, Oracle recommends that you use the OracleTextSearch option for full-text search. Note that this option should only be used in conjunction with an Oracle database.</p>	<p>See Section 11.2.3.8, "Enabling OracleTextSearch."</p> <p>For more information, also see the section "Configuring Oracle Text Search for Oracle Content Server" in <i>Oracle WebCenter Content Installation Guide</i> and the section "Site Studio Integration" in <i>Oracle WebCenter Application Administrator's Guide for Content Server</i>.</p>
Create Content Profiles	<p>Optional</p> <p>When iFraming is enabled in a WebCenter Portal application, users have the option to upload content based on Content Server Profiles</p>	<p>See Section 11.2.3.9, "Creating Content Profiles in Content Server."</p> <p>For more information about creating content profiles, see the chapter "Managing Metadata" in the <i>Oracle WebCenter Application Administrator's Guide for Content Server</i>.</p>
Configure Item Level Security	<p>Optional</p> <p>The Documents service can use Item Level Security (ILS) to override the default Spaces document security model, or to expose Content Server document security in a Framework application. Using ILS allows Content Server folders (and their children) or individual documents to have unique security permissions.</p>	<p>See Section 11.2.3.10, "Configuring Item Level Security in WebCenter Portal Applications."</p> <p>See also, "Setting Security Options on a Folder or File" in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces</i></p>
Additional Optional Configurations	<p>Optional</p> <p>After completing the rest of your configuration, you can optionally configure the FileStore Provider component and set up Node Manager.</p>	<p>See Section 11.2.3.11, "Additional Optional Configurations."</p>
Configure Security between Content Server and Framework applications	<p>Mandatory for Framework applications (not applicable to Spaces)</p> <p>To configure Content Server to work with a Framework application, you must first set up content security and users in a development environment and then migrate them to a production environment.</p>	<p>See Section 11.2.3.12, "Configuring Security Between Content Server and WebCenter Portal: Framework Applications."</p>

Table 11–1 (Cont.) WebCenter Portal-specific Configuration Tasks for Content Server

Task	Description	Documentation
Register the Content Server Connection	Mandatory For Framework applications, you must configure the connection from the application to Content Server. For Spaces, although in most cases the connection will be configured when Spaces first starts up, you should at least test it to make sure it has been configured correctly for your environment, and that data has been correctly seeded.	For Framework applications, see Section 11.2.3.13.1, "Configuring the Content Server Connection for Framework Applications." For Spaces, see Section 11.2.3.13.2, "Configuring the Content Server Connection for Spaces." For Spaces, be sure to also check the seeded data as described in Section 11.2.3.13.3, "Checking the Spaces Data Seeded in Content Server."

11.2.3 Configuring Content Server for WebCenter Portal Applications

After installing or upgrading to Content Server 11g, perform the configuration tasks listed in [Table 11–1](#). Unless otherwise noted, these tasks are common to both Spaces and Framework applications.

Note: Prior to beginning the configuration you must have completed the installation and configuration steps described in [Section 11.2.1, "Prerequisites to Configuring Content Server"](#) that define the starting point for the configuration steps in this section.

This section includes the following subsections:

- [Section 11.2.3.1, "Enabling Mandatory Components"](#)
- [Section 11.2.3.2, "Configuring the Dynamic Converter Component"](#)
- [Section 11.2.3.3, "Configuring the Inbound Refinery"](#)
- [Section 11.2.3.4, "Setting Up SSL for Content Server"](#)
- [Section 11.2.3.5, "Enabling the iFraming UI in WebCenter Portal"](#)
- [Section 11.2.3.6, "Configuring the SES Crawler"](#)
- [Section 11.2.3.7, "Setting Up Site Studio"](#)
- [Section 11.2.3.8, "Enabling OracleTextSearch"](#)
- [Section 11.2.3.9, "Creating Content Profiles in Content Server"](#)
- [Section 11.2.3.10, "Configuring Item Level Security in WebCenter Portal Applications"](#)
- [Section 11.2.3.11, "Additional Optional Configurations"](#)
- [Section 11.2.3.12, "Configuring Security Between Content Server and WebCenter Portal: Framework Applications"](#)
- [Section 11.2.3.13, "Registering the Content Server Connection"](#)

11.2.3.1 Enabling Mandatory Components

Mandatory

Follow the steps below to enable components required by Content Server. This includes Making sure that the `FrameworkFolders` folders component (which is not compatible with the `Folders_g` component) is disabled, enabling the `Folders_g` component (which provides a hierarchical folder interface to content in Content Server), and enabling the `WebCenterConfigure` component (which configures an instance of Content Server for WebCenter Portal applications). For more information about what the `WebCenterConfigure` component does, see [Section 11.2.3.1.1, "What You Should Know About the WebCenterConfigure Component."](#)

To enable required components:

1. Log onto the Administration server and open the Admin Server page.
You can access the Admin Server page through Content Server by going to **Administration > Admin Server**.
2. Click **Component Manager**.
The Component Manager page displays.
3. Make sure that the **FrameworkFolders** checkbox is unchecked.
4. Check the **WebCenterConfigure** checkbox and any other components that you want to enable.

On the Component Manager page, make sure that the **InboundRefinerySupport** checkbox is checked if you have installed and plan to use the Inbound Refinery. If you plan to use the **Dynamic Converter**, you can also select it here as you'll otherwise need to enable it later.

5. Click **Update**.
6. Click **Advanced Component Manager**.
The Advanced Component Manager page displays.
7. Select `Folders_g` in the **Disabled Components** list box and click **Enable**.
8. Restart the Content Server instance.

11.2.3.1.1 What You Should Know About the WebCenterConfigure Component

Enabling the `WebCenterConfigure` component performs the following tasks ([Table 11–2](#)) in Content Server:

Table 11–2 Tasks Associated with the WebCenterConfigure Component

Tasks	Pointers to Verify the Completion of Tasks
Enables accounts	Content Server > Administration > Admin Server > General Configuration > Enable Accounts checkbox or <code>FMW_HOME/user_projects/domains/ucm_domain/ucm/cs/config/config.cfg</code> file. The setting in this file is <code>UseAccounts=1</code> .
Allows updates to documents that are yet to be released	Content Server > Administration > Admin Server > General Configuration > Additional Configuration Variables or <code>FMW_HOME/user_projects/domains/ucm_domain/ucm/cs/config/config.cfg</code> The setting is <code>AllowUpdateForGenwww=1</code>

Table 11-2 (Cont.) Tasks Associated with the WebCenterConfigure Component

Tasks	Pointers to Verify the Completion of Tasks
Disables the cache for folders	<p>If the <code>Folders_g</code> component is enabled, <code>CollectionUseCache</code> is set to <code>false</code> by the <code>WebCenterConfigure</code> component each time the server starts up. This setting is visible in Administration > System Audit Information > Configuration Entry Information > Click All Environment Keys > shows all environment settings.</p> <p>or</p> <p>See the <code>FMW_HOME/user_projects/domains/ucm_domain/ucm/cs/config/config.cfg</code> file.</p> <p>The setting is <code>CollectionUseCache=1</code>.</p>
Adds metadata fields: <ul style="list-style-type: none"> ■ <code>xWCTags</code> ■ <code>xWCPageId</code> ■ <code>xCWWorkflowAssignment</code> ■ <code>xCWWorkflowApproverUserList</code> 	You can view, edit, and add metadata fields here: Content Server > Administration > Admin Applets > Configuration Manager > Information Fields tab.
Sets Folder settings if the <code>Folders_g</code> component is enabled: <ul style="list-style-type: none"> ■ System Default Information Field Configuration: Doc Type = Document ■ Information Field Inherit Configuration <code>xCWWorkflowAssignment</code> <code>xCWWorkflowApproverUserList</code>	Content Server > Administration > Folder Configuration > System Default Information Field Configuration Content Server > Administration > Folder Configuration > Information Field Inherit Configuration
Adds the <code>WCWorkflowApproverUserToken</code> workflow token	Content Server > Administration > Admin Applets > Workflow Admin > Options > Tokens menu
Adds three <code>DynamicConverter</code> templates	If the <code>DynamicConverter</code> component is enabled, the <code>DynamicConverter</code> service is called to create the three <code>DynamicConverter</code> templates: <ul style="list-style-type: none"> ■ <code>SLIDE-PREVIEW</code> ■ <code>SLIDE-PREVIEW-TEXT</code> ■ <code>SLIDE-PREVIEW-LARGE</code>

Table 11–2 (Cont.) Tasks Associated with the WebCenterConfigure Component

Tasks	Pointers to Verify the Completion of Tasks
<p>Overrides certain behavior of the Site Studio Switch Content wizard to make Site Studio work in the WebCenter Portal environment</p>	<p>This provides access to the Site Studio Switch Content wizard and the Site Studio Contributor editor from within Content Presenter to allow for adding and editing Site Studio documents from WebCenter Portal.</p> <ul style="list-style-type: none"> ▪ The contentwizard.hcsp and contentwizard.js files are copied from the /WebCenterConfigure.zip/component/WebCenterConfigure/publish/contentwizard/ directory to the OCS_HOME/cs/weblayout/resources/wcm/custom/sitestudio/contentwizard/webcenter/ directory. ▪ The wcm.sitestudio.form.js file is copied from the /WebCenterConfigure.zip/component/WebCenterConfigure/publish/contentwizard/directory to the OCS_HOME/cs/weblayout/resources/wcm/custom/sitestudio/ directory.
<p>Upgrades the PersonalSpace role and default attributes to 11.1.1.6.0 format</p>	<p>If Content Server contains an older version (11.1.1.5.0 and earlier) of the PersonalSpace role format, then enabling WebCenterConfigure upgrades the PersonalSpace role and default attributes to 11.1.1.6.0 format</p> <p>11.1.1.5.0 and earlier format:</p> <p>Roles:</p> <ul style="list-style-type: none"> ▪ PersonalSpaceRole with RWD permissions on the PersonalSpaces security group <p>Default Attributes:</p> <ul style="list-style-type: none"> ▪ All users (public and authenticated) get the PersonalSpaceRole <p>11.1.1.6.0 format:</p> <p>Roles:</p> <ul style="list-style-type: none"> ▪ PersonalSpaceRole with R permission on the PersonalSpaces security group ▪ PersonalSpaceAuthenRole with RWD on the PersonalSpaces security group <p>Default Attributes:</p> <ul style="list-style-type: none"> ▪ All public users get the PersonalSpaceRole ▪ All authenticated users get the PersonalSpaceAuthenRole

11.2.3.2 Configuring the Dynamic Converter Component

Optional, but strongly recommended

This configuration is required for the Slide Previewer capability in WebCenter Portal, which makes use of the HTML renditions generated on the fly by the Dynamic Converter.

The configuration for the Dynamic Converter consists of two steps: enabling the Dynamic Converter, and defining the file types for which the Dynamic Converter is available. If you enabled the Dynamic Converter previously when you were enabling the mandatory components, you can skip the steps to enable it and go directly to the steps for defining the file types.

Enabling the Dynamic Converter

To enable the Dynamic Converter:

1. Log onto the Administration server and open the Admin Server page.
You can access the Admin Server page through Content Server by going to **Administration > Admin Server**.
2. On the Component Manager page check the **DynamicConverter** checkbox.
3. Click **Update**.
4. Restart the Content Server instance.

Setting the file types to be sent to the Dynamic Converter

To define the file types for which Dynamic Converter is available:

1. Log in to the Content Server and select **Administration > Dynamic Converter Admin > Configuration Settings > Conversion Formats**.

Note that the Dynamic Converter Admin menu option will not be visible until after you restart the Content Server instance after enabling the Dynamic Converter component.

2. Select the file formats from the dropdown list for which the Dynamic Converter will be enabled. Choose all the document formats for which you want HTML renditions such as Word, Excel, PowerPoint, and PDF.

11.2.3.3 Configuring the Inbound Refinery

Optional, but strongly recommended

The Inbound Refinery is a conversion server that manages file conversions for electronic assets such as documents, digital images, and motion videos. It also provides thumbnail functionality for documents and images and storyboarding for videos. You can use Inbound Refinery to convert content items stored in Content Server.

To configure Inbound Refinery, you must set up an outgoing provider from Content Server to Inbound Refinery, and specify the file types that will be converted. You also need to enable PDFExportConverter and set other conversion settings on Inbound Refinery. Although optional, you may also want to enable the conversion of wikis and blogs to PDF.

Prior to configuring Inbound Refinery, you should have:

- Installed Inbound Refinery, as described in [Section 11.2.1.1, "Installation Prerequisites"](#)
- Completed the initial post-install configuration as described in [Section 11.2.1.2, "Configuration Prerequisites"](#)
- Checked that the `InboundRefinerySupport` component is enabled as described in [Section 11.2.3.1, "Enabling Mandatory Components"](#)

This section contains the following subsections:

- [Section 11.2.3.3.1, "Creating an Outbound Provider"](#)
- [Section 11.2.3.3.2, "Enabling PDFExportConverter in Inbound Refinery"](#)
- [Section 11.2.3.3.3, "Selecting the File Formats To Be Converted"](#)
- [Section 11.2.3.3.4, "Enabling the Conversion of Wikis and Blogs into PDFs"](#)

11.2.3.3.1 Creating an Outbound Provider

Before Content Server can send files to Inbound Refinery for conversion, you must set up an outgoing provider from Content Server to Inbound Refinery with the **Handles Inbound Refinery Conversion Jobs** option checked.

To create an outbound provider:

1. From the Content Server Administration menu, choose **Providers**.
 2. In the Create a New Provider section of the Providers page, click **Add** in the outgoing row.
 3. Enter values for these fields:
 - **Provider Name:** Any short name with no spaces describing the Inbound Refinery instance the outgoing provider is for. It is a good idea to use the same name as the Inbound Refinery **Instance Name**.
 - **Provider Description:** A description of the outgoing provider.
 - **Server Host Name:** The name of the host machine where the Inbound Refinery instance is running (for example, `myhost.example.com`).
 - **HTTP Server Address:** The address of the Inbound Refinery instance (for example, `http://myhost.example.com:16250` where 16250 is the Web port).
 - **Server Port:** The `IntradocServerPort` value for the Inbound Refinery instance. This value was entered on the post-installation configuration page, and can be found on the Inbound Refinery configuration information page under **Server Port**. You can also find it in the `FMW_HOME/user_projects/domains/ucm_domain/ucm/ibr/config/config.cfg` file as `IntradocServerPort`.
- To display the Inbound Refinery configuration information page:
- Log in to the Content Server and choose **Administration > Configuration for <instanceName>**.
 - Click **Server Configurations** to display the server configurations.
- **Instance Name:** The instance name for Inbound Refinery (the `IDC_Name` value in the `config.cfg` file). This value was entered on the post-installation configuration page as **Server Instance Name**, and can be found on the Inbound Refinery configuration information page.
 - **Relative Web Root:** The web root of the Inbound Refinery instance (for example, `/ibr/`).
4. Under Conversion Options, check **Handles Inbound Refinery Conversion Jobs**. Do *not* check **Inbound Refinery Read Only Mode**.
 5. Click **Add**.
 6. Restart Content Server.
 7. Go back to the Providers page, and check that the Connection State value is good for the provider.

If the value is not good, double-check that you entered all the preceding entries correctly, and check that the Content Server and Inbound Refinery instances can ping each other.

11.2.3.3.2 Enabling PDFExportConverter in Inbound Refinery

PDFExportConverter uses OutsideIn to convert documents directly to PDF files. The conversion can be cross-platform and does not require any third-party product. You can enable PDFExportConverter for Inbound Refinery as a server feature.

To enable PDFExportConverter on Inbound Refinery:

1. From the Inbound Refinery Administration menu, select **Admin Server** and then **Component Manager**.
2. Select PDFExportConverter, and click **Update**.
3. Click **OK** to enable this feature.
4. Restart Inbound Refinery.

To set the PDF converter settings:

1. Log in to Inbound Refinery again.
2. Select **Conversion Settings**, then select **Primary Web Rendition**.
3. Check **Convert to PDF using PDF Export**.
4. Select **Conversion Settings**, then select **Additional Renditions**.
5. Check **Create Thumbnail Images using Outside In**.
6. Select **Conversion Settings > Third Party Application Settings > General OutsideIn Filter Options > Options**.
7. Set the **Path to fonts** to the fonts on the Inbound Refinery system.
8. Select **Use internal graphics rendering** under UNIX Rendering Options.
9. Click **Update**.

For more information, see "Setting PDF Files as the Primary Web-Viewable Rendition" in *Oracle Fusion Middleware Administrator's Guide for Conversion*.

11.2.3.3.3 Selecting the File Formats To Be Converted

To tell Content Server which files to send to Inbound Refinery to be converted, you need to select the file formats.

To select the file formats to be converted:

1. From the Content Server Administration menu, choose **Refinery Administration** and then **File Formats Wizard**.

Note: **Refinery Administration** is not listed when there is no valid outgoing provider to an Inbound Refinery instance, or the InboundRefinerySupport component is not enabled.

Content Server displays the File Formats Wizard page. This page configures which file formats will be sent to Inbound Refinery for conversion when they are checked into Content Server.

2. Select the formats you want converted.

Make sure you check all the file types you want sent to Inbound Refinery for conversion. Do *not* to check HTML, and also do not check **wiki** and **blog** unless you have enabled their conversion through the **WebCenterConversions** component as described in [Section 11.2.3.3.4, "Enabling the Conversion of Wikis and Blogs into PDFs."](#)

3. Click **Update**.

11.2.3.3.4 Enabling the Conversion of Wikis and Blogs into PDFs

Optional

Before you can enable the conversion of wikis and blogs into PDFs in WebCenter Portal applications, you must first:

- Set up the OpenOffice integration with Inbound Refinery. For information, see "Setting PDF Files as the Primary Web-Viewable Rendition" in *Oracle Fusion Middleware Administrator's Guide for Conversion*.
- Perform the steps described in the section "Setting Classpath to OpenOffice Class Files" (see also: "Using OpenOffice Without Logging In to Host") in *Oracle Fusion Middleware Administrator's Guide for Conversion*.

Enabling the conversion of wikis and blogs into PDFs requires you to first install the WebCenterConversions component, then configure OpenOffice, which converts HTMLs to PDFs, in the Inbound Refinery server and Content Server respectively. The WebCenterConversions component adds the HtmToPDFOpenOffice conversion option, which makes use of OpenOffice conversion in Inbound Refinery (and therefore requires OpenOffice to be configured for that Inbound Refinery).

Note that you must complete the steps below in sequence. If you enable Wiki and Blogs by selecting them in the file Formats Wizard without first installing and enabling the Inbound Refinery the Wiki and Blogs documents will be stuck in the Inbound Refinery conversion queues.

Tip: See also, "File Formats Converted to PDF by Open Office" at *Oracle Fusion Middleware Administrator's Guide for Conversion*.

To install the WebCenterConversion component:

1. Log in to the Inbound Refinery server.
2. Click **Administration** and then select **Admin Server**.
The Inbound Refinery Admin Server page displays.
3. In the Component Manager, click the **advanced component manager** link.
The Advanced Component Manager page displays.
4. In the Install New Component section, select **WebCenterConversions.zip** from the companion CD, then click **Install**.
The WebCenterConversion component displays in the Disabled Components box.
5. Select **WebCenterConversion** and click **Enable**.
6. Restart the Inbound Refinery server.

To enable the WebCenterConversion component:

1. In the Inbound Refinery server, under **Conversion Settings**, click the **Conversion Listing** link.
This displays the Conversion Listing page.
2. In the **Conversions** table, select the **Accept** checkbox for `HtmToPDFOpenOffice`, and click **Update**.

The Wiki and Blog options will now appear in Content Server's File Formats Wizard in the associated Content Server instance.

To enable Wiki and Blogs to be converted to PDFs in Content Server:

1. Log in to Content Server.
2. Expand the **Administration** node, then **Refinery Administration**, and then click **File Formats Wizard**.
3. Under **Select File Types**, select the **Wiki** and **Blogs** checkboxes and click **Update**.

11.2.3.4 Setting Up SSL for Content Server

If the Spaces or Framework application and the Content Server you intend to create a repository connection to are not on the same system or the same trusted private network, then identity propagation is not secure. To ensure secure identity propagation you must also configure SSL for Content Server. For a step-by-step description of how to set up SSL for Content server, see [Section 33.7, "Securing the Spaces Connection to Content Server with SSL."](#)

11.2.3.5 Enabling the iFraming UI in WebCenter Portal

Optional, but strongly recommended

WebCenter Portal applications (that is Spaces and Framework applications) use Content Server UI presented in an iFrame for certain functionality, such as Document Manager document rendition and advanced metadata editing. iFrame does not support cross-domain communications, so if the WebCenter Portal application and Content Server are not in the same domain (in terms of their web address) you must configure the Oracle HTTP Server (OHS), as described below, or iFraming functionality not be available.

Note: Before enabling support for iFraming, you should already have installed and configured the Oracle HTTP Server (OHS) as described [Section 31.2.5, "Installing and Configuring the Oracle HTTP Server."](#)

To enable the iFraming UI in the WebCenter Portal application:

1. Open the `mod_wl_ohs.conf` file and make sure it points to the right Content Server instance.

The default location of this file is:

```
OHS_HOME/Oracle_WT1/instances/instance1/config/OHS/ohs1/mod_wl_ohs.conf
```

2. Update the connection property of the Content Server to:

```
webContextRoot= '/cs'
```

Note that this setting should never be set if OHS is not set up or it is not working correctly.

3. If there is more than one Content Server, reconfigure the second one to use a different context root.
4. Configure OHS by updating the `mod_wl_ohs.conf` file with the Content Server and `adfAuthentication` protected URI information. For example:

```
<Location /cs>
SetHandler weblogic-handler
WeblogicHost example.com
WeblogicPort 9400
```

```
</Location>

<Location /adfAuthentication>
SetHandler weblogic-handler
WeblogicHost example.com
WeblogicPort 9400
</Location>
```

For more information about configuring OHS through the the `mod_wl_ohs.conf` file, see [Appendix B, "Oracle HTTP Server Configuration for WebCenter Portal."](#)

5. Open the Spaces or Framework application and check that the iFraming functionality is available.

Note that since the WebCenter Portal application is now front-ended by OHS, when you access Spaces or the Framework application you need to do so through OHS. Consequently, you would access your application using the following:

```
http://<host>:<OHSPort>/webcenter
```

For example:

```
http://example.com:7777/webcenter
```

11.2.3.6 Configuring the SES Crawler

Optional

Follow the steps in [Section 22.6.2, "Setting Up Oracle WebCenter Portal: Content Server for Oracle SES Search"](#) to configure the SES crawler.

11.2.3.7 Setting Up Site Studio

Optional, but recommended

Configuring Site Studio is optional, but without it you will not be able to create and use Site Studio-related assets in Content Presenter.

To enable Site Studio:

1. Log in to Content Server and open the Admin Server Page.

The Component Manager Page displays.

2. Click **All Features**.

All components from the Document Management, Folders, Inbound Refinery, Integration, and Web Content Management categories are displayed.

3. Select the checkbox for each component you want to enable. The following components should be enabled:

- LinkManager
- SiteStudio
- SiteStudioExternalApplications
- DBSearchContainsOpSupport (not required for Oracle Text Search)

Site Studio supports either Oracle Text Search or Full Text Search (Metadata search is not supported). If Oracle Text Search is configured, then `DBSearchContainsOpSupport` should not be enabled. However, if Full Text Search is configured, then `DBSearchContainsOpSupport` must be enabled for Site Studio Designer to work properly.

4. Click **Update**.
5. Restart the Content Server instance.
6. Log back into Content Server and open the Administration page.
7. Select Site Studio Administration, and then Set Default Project Document Information.
8. Accept the defaults and click **Update**.
9. Select Site Studio Administration, and then Set Default Web Asset Document Information.
10. Accept the defaults and click **Update**.
11. To use the Site Studio Designer, log into the Content Server console and navigate to `my_downloads`, download Site Studio Designer and install it.

11.2.3.8 Enabling OracleTextSearch

Optional, but recommended

Although optional, for full-text search, Oracle recommends that you use the OracleTextSearch option. By default, the database used by Content Server is set up to provide metadata-only searching and indexing capabilities. However, you can modify the default configuration of the database to additionally support full-text searching and indexing.

Note that this option should only be used in conjunction with an Oracle database; the OracleTextSearch index must always be in an Oracle database, regardless of the database type used for the main schema. For more information, see the section "Configuring Oracle Text Search for Oracle Content Server" in *Oracle WebCenter Content Installation Guide*, and the section "Site Studio Integration" in *Oracle WebCenter Application Administrator's Guide for Content Server*.

11.2.3.9 Creating Content Profiles in Content Server

Optional

When iFraming is enabled in a WebCenter Portal application, users have the option to upload content using Content Server Profiles. For more information on Content Server Profiles, see "Using Profiles to Customize Content Screens" in the *Oracle WebCenter Application Administrator's Guide for Content Server*.

The fields described in the section "Content Check-In Form" (see the table) in the "User Interface" appendix in the *Oracle WebCenter User's Guide for Content Server* are mandatory for Content Server. All content profiles must include them, otherwise the check-in will fail. As indicated in the table, some fields can be added as hidden or information fields to the profile.

In addition to the mandatory fields needed to upload files to Content Server, for the upload profiles to work correctly in Document Library and Spaces, the Content Server profiles should also contain the following fields:

- **xCollectionID** - for the folder name to be persisted
- **xIdcProfile** - for the profile value to be persisted
- **dRevLabel** - required by the CHECKIN_SEL_FORM API to enable a new version to be checked in

These fields can be added as hidden fields to the profile.

11.2.3.10 Configuring Item Level Security in WebCenter Portal Applications

Optional

The Documents service can use Item Level Security (ILS) to override the default Spaces document security model, or to expose Content Server document security in a Framework application. Using ILS allows Content Server folders (and their children) or individual documents to have unique security permissions.

This section includes the following sections:

- [Section 11.2.3.10.1, "What You Should Know About Item Level Security."](#)
- [Section 11.2.3.10.2, "Configuring Item Level Security"](#)
- [Section 11.2.3.10.3, "Configuring Additional Settings for WebCenter Portal: Framework Applications"](#)

11.2.3.10.1 What You Should Know About Item Level Security

Oracle WebCenter Portal allows custom permissions to be set on a file or a folder. This feature is referred to as Item level Security (ILS). Once configured, the feature can be accessed from the WebCenter Portal Administration Console by selecting **File > Security** when viewing a file or folder (see [Section 36.6.1, "Managing Content"](#)).

Note: In Spaces, using ILS as the primary security mechanism for a space may become difficult to administer when the number of users grow. Moreover, ILS may not be as efficient as the Spaces security model. Therefore, Oracle recommends using ILS only to define security for the documents or folders that do not fit within the Spaces security model. For example, documents and folders to which only a restricted set of users have access. For information about security, see the section "Managing Roles and Permissions for a Space" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

ILS can be used to replace the existing file or folder security with a custom set of permissions.

- When applied to a file, the custom permissions affect only that file.
- When applied to a folder, the updated security is propagated to all child files and folders recursively, stopping when a folder is encountered with its own custom permissions. The propagation does not affect a file with its own custom permissions, if already set.

Note: ILS cannot be applied to the root folder of a space in the Spaces application. This is so that the space's security can be correctly restored on a file or folder when its item level security is removed.

Within the Content Server, ILS is implemented as a combination of ACL, account, and other metadata field settings. Content Server must be correctly configured to enable ILS. See, [Section 11.2.3.10, "Configuring Item Level Security in WebCenter Portal Applications"](#) and [Section 11.2.3.12, "Configuring Security Between Content Server and WebCenter Portal: Framework Applications."](#)

What Happens in Content Server on Setting Custom Permissions

The following occurs in Content Server on setting custom permissions for a file or folder from the Item Level Security dialog:

- The account is changed to account `WCILS/original_account`.
All AUTHENTICATED users are by default granted RWDA on account WCILS, and all PUBLIC users are granted R on the account WCILS. Changing the account to `WCILS/original_account` ensures that only the custom permissions determine the security on the content.
- The ACL content metadata fields, `xClbraUserList` and `xClbraRoleList` are updated with the custom permissions. (`xClbraUserList` contains the permissions a user has on a document or folder, and `xClbraRoleList` contains the permissions a group has on the document or folder.)
- The content metadata field, `xInhibitUpdate` is set to `true`, to prevent ILS from overwriting an item's own custom security with a parent folder's custom permissions.

What Happens in Content Server on Removing Custom Permissions

Removing custom permissions from a folder or file attempts to revert the security on that item to the security set on the item's parent folder. When you remove custom permissions, the following changes take place within Content Server:

- The item's account is changed to be the account of its parent folder.
- The item's ACL content metadata fields, `xClbraUserList` and `xClbraRoleList` are cleared.
- The content metadata field, `xInhibitUpdate` is set to `false`.

These changes are propagated in the same way as when the item level security is set.

Prerequisites for Using Item Level Security in WebCenter Portal: Framework Applications

For a WebCenter Portal application, the Item Level Security (ILS) feature is supported only if the application's Content Server security configuration meets certain prerequisites. In most scenarios ILS is not required, and therefore, it should not be enabled unless explicitly needed. Typical reasons for using ILS are application situations when the Content Server security models need to be overridden or supplemented to handle exception cases to security policies for individual users or groups of users, on a per document basis. Please be aware that there are performance impacts and additional administrative overhead when using ILS.

Note: Oracle recommends using Content Server security because it is efficient and scales easily for a large number of users and content objects compared with item level security. From an administrative perspective, Content Server's security is also easier to maintain. For information about configuring security, see [Section 11.2.3.12, "Configuring Security Between Content Server and WebCenter Portal: Framework Applications."](#)

The following are the Content Server security ILS prerequisites for a WebCenter Portal application:

- Security is based on Content Server *Accounts* alone.

Since all content must also have a security group, this means all application users must have RWD permissions granted to the application's security group. This is necessary because of how ILS works, that is, on setting the custom permissions, the account automatically changes to `WCILS/original_account`, which is an account all users have RWDA granted to. This is so that the custom permissions alone determine the security on the document or folder.

- The content metadata field, `xForceFolderSecurity` is set to `true` for the entire application content. That is, `Folder` security settings are enforced on child folders and documents. This is necessary to support the propagation of custom permissions.

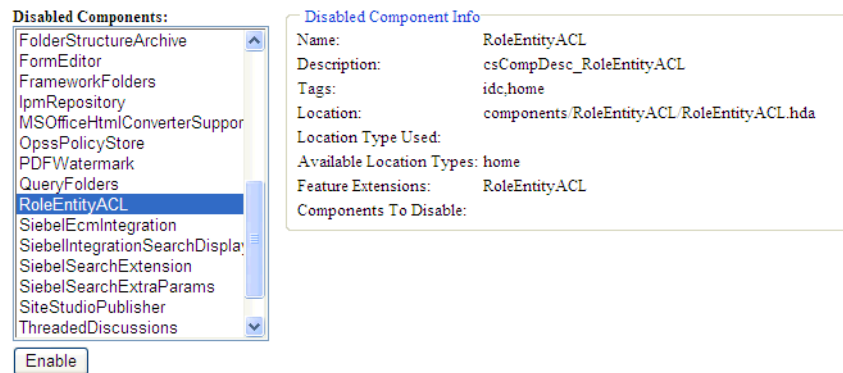
11.2.3.10.2 Configuring Item Level Security

To configure Item Level Security (ILS):

1. Log on to your Content Server instance.
2. From the Administration menu, choose **Admin Server** to open **Component Manager**.
3. In the **Component Manager** section, click the **Advanced Component Manager** link.
4. In the Advanced Component Manager page, scroll down to the **Disabled Components** list, select **RoleEntityACL**, as shown in [Figure 11-2](#), and then click **Enable**.

See Also: "Setting Security Options for a File" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

Figure 11-2 Advanced Component Manager - RoleEntityACL Component



5. From the **Options** pane on left, select **General Configuration**.
6. Under the General Configuration page, in the **Additional Configuration Variables** box, add the following parameters:

```
UseEntitySecurity=1
SpecialAuthGroups=PersonalSpaces,securityGroup
```

where:

`SpecialAuthGroups` is a comma separated list (no spaces allowed between values) of security groups. The ILS option is enabled only on content in these security groups.

- For WebCenter Portal applications, the *securityGroup* is the name of the security group in which content is created.
- For Spaces, the name of the security group that contains the Spaces data is the same as the Document Spaces properties application name. You can find the application name using either Fusion Middleware Control or WLST.

In Fusion Middleware Control, the application name is displayed as part of the Content Server default connection in the Spaces connections.

In WLST, the application name is shown using the `listDocumentsSpacesProperties` command. For example:

```
listDocumentsSpacesProperties('webcenter')
```

```
The Documents Spaces container is "/myspacesroot"
The Documents repository administrator is "weblogic"
The Documents application name is "myspacesapp" <- applicationName
The Documents primary connection is "myucm"
```

7. Restart Content Server.

11.2.3.10.3 Configuring Additional Settings for WebCenter Portal: Framework Applications

For a Framework application, in addition to the steps described in [Section 11.2.3.10.2, "Configuring Item Level Security"](#), ensure that all users by default are granted RWDA on the WCILS account. To do this, use the SET_DEFAULT_ATTRIBUTES service. For information about the SET_DEFAULT_ATTRIBUTES service, see the section "SET_DEFAULT_ATTRIBUTES" in *Oracle WebCenter Content Services Reference Guide*.

To run the SET_DEFAULT_ATTRIBUTES service through a browser:

1. From a browser, log into Content Server as an administrative user.
2. View the source for the page, and find the value of the idcToken by searching for a line containing `var idcToken =` (for example, `var idcToken = 1316188662243:6FE5F809A3B122277B7A1D19912FBB5`).
3. While in the same browser window, enter the URL in the format:

```
http://host:port/cs/idcplg?IdcService=SET_DEFAULT_ATTRIBUTES&dECPropSubKey=<Security Group>&dDefAttribs=account,WCILS,15&idcToken=<idcToken>&IsSoap=1
```

For example:

```
http://myhost.com:4444/cs/idcplg?IdcService=SET_DEFAULT_ATTRIBUTES&dECPropSubKey=Custom&dDefAttribs=account,WCILS,15&idcToken=1291297336399:6E324367FC9D2F8BE525F4CEBF4463FC&IsSoap=1
```

11.2.3.11 Additional Optional Configurations

This section describes additional optional configurations that are not required for Content Server to function correctly, but nonetheless offer value and comprise best practices for a Content Server enterprise installation.

This section includes the following subsections:

- [Section 11.2.3.11.1, "Configuring the File Store Provider"](#)
- [Section 11.2.3.11.2, "Setting Up Node Manager"](#)

11.2.3.11.1 Configuring the File Store Provider

A file store for data management is used in the Content Server system instead of the traditional file system for storing and organizing content. The File Store Provider component is installed, enabled, and upgraded by default for a new Content Server instance (with no documents in it). The File Store Provider component automatically upgrades the default file store (DefaultFileStore) to make use of functionality exposed by the component, including modifying the web, vault, and web URL path expressions.

The File Store Provider component exposes the file store functionality in the Content Server interface and allows additional configuration options. For example, you can configure the Content Server instance to use binary large object (BLOB) data types to store content in a database, instead of using a file system.

With File Store Provider, checked-in content and associated metadata are examined and assigned a storage rule based on criteria established by a system administrator. Criteria can include metadata, profiles, or other considerations. The storage rule determines how vault and web files are stored by the Content Server system and how they are accessed by a web server.

The File Store Provider component enables you to define data-driven rules to store and access content managed by the Content Server system. The configuration steps below create a storage rule that ensures content is stored in the database rather than on the file system.

To create a storage rule:

1. Log in to the Content Server instance as system administrator.
2. Select **Administration**, then **Providers**.
The Providers Page displays.
3. Click **Info** in the Action column next to the `DefaultFileStore` provider.
The File Store Provider Information Page displays.
4. Specify a name for the rule (for example, `DBStorage`) and select **JDBC Storage**.
5. Click **OK**.
The Edit File Store Provider Page displays.
6. Click **Update**.
7. Restart the Content Server instance.

11.2.3.11.2 Setting Up Node Manager

As an additional step to configuring and managing Content Server and the other servers in the domain in which it resides, you may want to consider using Oracle WebLogic Server Node Manager. Node Manager lets you start and stop WebLogic Server instances remotely, monitor them, and automatically restart them after an unexpected failure. You can configure Content Server, the Administration Server, and Node Manager to work together in a WebLogic Server domain. Node Manager is installed on all the machines that host any server instance. For more information about using Node Manager, see “Using Node Manager with Oracle WebCenter Content” in the *Oracle WebCenter Content Installation Guide*.

11.2.3.12 Configuring Security Between Content Server and WebCenter Portal: Framework Applications

Mandatory for Framework applications

To configure Content Server to work with a Framework application, you must first set up content security and users in a development environment and then migrate them to a production environment. For detailed information about security, see also the chapter "Managing Security and User Access" in *Oracle WebCenter Content System Administrator's Guide for Content Server*.

This section describes the following mandatory steps:

- **Creating security groups:** All content items, whether that be a folder or a document, must reside in a security group. Security groups are required for folders so the folder content can be restricted or its access can be customized based on who should view, edit, or manage the folder content. To create security groups follow the steps in [Section 11.2.3.12.1, "Creating a Security Group Using the Content Server Console."](#)
- **Creating roles:** Roles are created with different permissions such as, read, write, delete, administer, and are used to define permissions on security groups. First you must create roles in Content Server, as described in [Section 11.2.3.12.2, "Creating Roles Using the Content Server Console"](#) and then for the WebCenter Portal application, as described in [Section 11.2.3.12.3, "Creating Roles \(Groups\) Using Fusion Middleware Control."](#)
- **Creating folders:** Folders include content such as files, subfolders, images. To create folders, follow the steps in [Section 11.2.3.12.4, "Creating a Folder Using the Content Server Console."](#)
- **Creating users:** Users are assigned different roles based on their roles and responsibilities in their organizations. Create users as described in [Section 11.2.3.12.5, "Creating Users Using Fusion Middleware Control"](#) and then grant roles to these users, as described in [Section 11.2.3.12.6, "Granting a Role to a User Using Fusion Middleware Control."](#)
- **Migrating security:** Migrate these security groups, folders, users, and roles to your production environment. For information, see [Section 11.2.3.12.7, "Migrating Security to a Production Environment."](#)
- **Checking the configuration:** check that the security groups and roles have been created correctly as described in [Section 11.2.3.12.8, "Checking Your Security Group and Roles Configuration."](#)

The procedures described in this section apply to the Documents service (including wikis and blogs) and Content Presenter.

11.2.3.12.1 Creating a Security Group Using the Content Server Console

To create a security group:

1. Log into the Content Server Console as an administrator.
2. From the Administration menu, choose **Admin Applets**.
3. On the Administration Applet page, click **User Admin** to display the User Admin dialog.
4. From the Security menu, choose **Permissions by Group**.
5. In the Permission By Group dialog, click **Add Group**.
6. In the Add New Group dialog, enter a group name, for example, WikiBlog.
7. Click **OK**.

The security group, which you will use when you create a folder in [Section 11.2.3.12.4, "Creating a Folder Using the Content Server Console,"](#) is created.

11.2.3.12.2 Creating Roles Using the Content Server Console

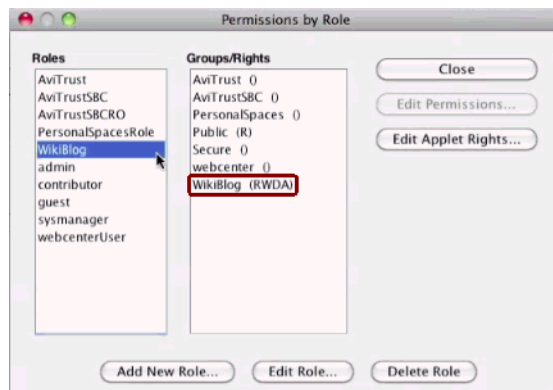
This section describes how to set up two roles in Content Server that mimic those you'll set up in the Framework application: one granting only read permission to the security group, and another granting all permissions to the security group.

To create roles:

1. Log into the Content Server Console as an administrator.
2. From the Administration menu, choose **Admin Applets**.
3. On the Administration Applet page, click **User Admin** to display the User Admin dialog.
4. Create a new role with full access:
 - a. From the Security menu, choose **Permissions by Role**.
 - b. In the Permission By Group dialog, click **Add New Role**.
 - c. In the Add New Role dialog, enter a name, for example, `WikiBlog`.
 - d. Click **OK**. This displays the Permission By Role dialog.
 - e. In the Groups/Rights column, select the security group that you created earlier (for example, `WikiBlog`), as described in [Section 11.2.3.12.1, "Creating a Security Group Using the Content Server Console."](#)
 - f. Click **Edit Permissions**.
 - g. In the Edit Permissions dialog, select all checkboxes: Read, Write, Delete, and Admin, and click **OK**.

RWDA access is enabled, as shown in [Figure 11-3](#).

Figure 11-3 RWDA Permissions



5. Create another role (for example `WikiBlogRO`) with only Read access following steps [4a](#) to [4f](#) and selecting the **Read** checkbox in the Edit Permissions dialog in step [4g](#).

11.2.3.12.3 Creating Roles (Groups) Using Fusion Middleware Control

This section steps you through creating two roles in the Framework application: one role with read access, and another with full access (read, write, delete, administer) .

To create roles (groups):

1. Log into Fusion Middleware Control as an administrator.

2. Under **Domain Structure**, click **Security Realms**.
3. In the table under the Summary of Security Realms section, click **myrealm**, for example.
IMPORTANT: **myrealm** uses the embedded LDAP that ships with Oracle WebCenter Portal. If your installation uses a different LDAP, you must select that instead of the embedded LDAP.
4. Select the **Users and Groups** tab and then the **Groups** subtab.
5. Under the **Groups** section, click **New** to display the Create a New Group section.
6. In the **Name** field, enter the name of the role to which you granted full access in Content Server (for example, `WikiBlog`), as described in [Section 11.2.3.12.2, "Creating Roles Using the Content Server Console"](#), and click **OK**.
7. Create a role or group with the read permission (for example, `WikiBlogRO`) by performing steps 5 and 6. The name of this role must match that you specified in Content Server, as described in [Section 11.2.3.12.2, "Creating Roles Using the Content Server Console."](#)

11.2.3.12.4 Creating a Folder Using the Content Server Console

To create a folder:

1. Log into the Content Server Console as an administrator.
2. From the Browse Content menu, choose **Contribution Folders** to display the root directory in which you will create a folder.
3. On the Contribution Folders page, from the New Item menu, choose **New Folder** to display the Hierarchy Folder Configuration page.
4. In the **Virtual Folder Name** field, enter a meaningful name (for example `WikiBlog`).
5. Under the Folder Information section, in the **Title** field, enter a meaningful title (for example, `WikiBlog`).
6. From the Security Group dropdown, select the security group that you created as described in [Section 11.2.3.12.1, "Creating a Security Group Using the Content Server Console."](#)

All items in this folder will inherit the security from this security group.

7. Click **Save**.

11.2.3.12.5 Creating Users Using Fusion Middleware Control

This section steps you through creating two users: a user for the read role, and a role for the full access (read, write, delete, administer) role.

To create users:

1. Log into Fusion Middleware Control as an administrator.
2. Under Domain Structure, click **Security Realms**.
3. In the table under the Summary of Security Realms section, click **myrealm**, the built-in realm that works with the integrated LDAP.
4. Select the **Users and Groups** tab and then the **Users** subtab.
5. Under the **Users** section, click **New** to display the Create a New User section.
6. In the **Name** field, specify a name, for example `Joe`.

7. In the **Password** field, specify a password.
8. In the **Confirm Password** field, enter the password again, and then click **OK**.
9. Create another user by performing steps 4 to 8.

11.2.3.12.6 Granting a Role to a User Using Fusion Middleware Control

This section steps you through granting the roles you created in [Section 11.2.3.12.3, "Creating Roles \(Groups\) Using Fusion Middleware Control"](#) to the users you created in [Section 11.2.3.12.5, "Creating Users Using Fusion Middleware Control"](#).

To grant a role to a user:

1. Log into Fusion Middleware Control as an administrator.
2. Under Domain Structure, click **Security Realms**.
3. In the table under the Summary of Security Realms section, click **myrealm**, the built-in realm that works with the integrated LDAP.
4. Select the **Users and Groups** tab and then the **Users** subtab.
5. In the table under the Users section, click the name of the user you created in [Section 11.2.3.12.5, "Creating Users Using Fusion Middleware Control"](#), to display the settings section.
6. Select the **Groups** tab.
7. Under Parent Groups, in the Available column, select the role with the read permission (for example, `WikiBlogRO`) that you created in [Section 11.2.3.12.3, "Creating Roles \(Groups\) Using Fusion Middleware Control"](#).
8. Move this role to the Chosen column and click **Save**.
9. Repeat steps 5 to 8 and grant the role with the full access permission to another user you created.

11.2.3.12.7 Migrating Security to a Production Environment

For information about migrating security from a development environment to a production environment, see [Section 28.2.5, "Post-deployment Security Configuration Tasks."](#)

11.2.3.12.8 Checking Your Security Group and Roles Configuration

After completing your configuration, follow the steps below to check that the security group and roles have been created correctly, and that a root folder has been created.

To verify that the security group and roles have been created:

1. Log in to the Content Server Console as an administrator.
2. From the Administration menu, choose **Admin Applets**.
3. On the Administration Applet page, click **User Admin** to display the User Admin dialog.
4. From the Security menu, choose **Permissions by Group**.
5. In the Permission By Group dialog, make sure that the security group is listed in the Groups list. The name of the security group ID should be the same as the Application Name in the Spaces document properties.
6. Select the security group in the groups list.

7. Check that the Roles list contains the two roles: `<applicationName>User` and `<applicationName>AuthenUser` with R and RWD permissions for the group space respectively.

To verify that the root folder has been created:

1. Log in to the Content Server Console as an administrator.
2. From the Browse Content menu, check that the root folder is listed and select it.
3. Verify that the child folder `spacetemplate` is listed
4. Click **Info** to display the Hierarchical Folder Information screen.
5. Verify that the Security Group is correct.

11.2.3.13 Registering the Content Server Connection

Mandatory for Framework applications/Optional, but strongly recommended for Spaces

For Framework applications, before you can use the configured Content Server, you must configure the connection between the application and Content Server. For Spaces, although the connection should be configured for you when the application first starts up, you should at least test the connection and check that the expected data has been properly seeded.

This section includes the following subsections:

- [Section 11.2.3.13.1, "Configuring the Content Server Connection for Framework Applications"](#)
- [Section 11.2.3.13.2, "Configuring the Content Server Connection for Spaces"](#)
- [Section 11.2.3.13.3, "Checking the Spaces Data Seeded in Content Server"](#)

11.2.3.13.1 Configuring the Content Server Connection for Framework Applications

After installing and configuring Content Server, continue by configuring the connection between the Framework application and Content Server. For more information about configuring the connection, see [Section 11.6.2, "Registering Content Repositories Using Fusion Middleware Control"](#) or [Section 11.6.3, "Registering Content Repositories Using WLST."](#)

11.2.3.13.2 Configuring the Content Server Connection for Spaces

Although the connection between Spaces and Content Server should have automatically been configured when the application first starts up, you should at least test the connection and check that it has been appropriately configured for your environment. For high availability environments, or for single sign-on environments, you may have to modify the Spaces host and port settings.

After installing and configuring Content Server, and restarting Spaces, check that your Spaces connection to Content Server is properly configured as described in [Section 11.11.1, "Testing Content Server Connections."](#) If your connection was not properly configured, then configure it as shown in [Section 11.10, "Setting Connection Properties for the Spaces Content Repository."](#) Note that Content Server should always be up and running before a Spaces instance is restarted.

Some WebCenter Portal components, such as the Documents service, rely on the data seeded in Content Server when Spaces first starts up. Before configuring other components with Spaces, check that the expected data has been properly seeded as

described in [Section 11.2.3.13.3, "Checking the Spaces Data Seeded in Content Server."](#)
 Note also that

11.2.3.13.3 Checking the Spaces Data Seeded in Content Server

When Spaces first starts up, a set of default data is seeded in Content Server. The data seeded in Content Server for a Spaces instance is based on the Document Spaces properties for the active Content Repository Connection. For example:

```
Root folder = /WebCenter1
Application Name= WC1
```

If the data is not correct, or has only been partially seeded, check the Spaces log and your Content Server configuration, make the necessary corrections to the Document Spaces properties, and then restart the Spaces instance to reseed them. Note that Content Server should always be up and running before a Spaces instance is restarted. For information about setting the default content repository, and setting additional Document Spaces properties required for a Spaces content repository, see [Section 11.8, "Modifying Content Repository Connection Details."](#)

[Table 11–3](#) illustrates the Group Spaces data that is seeded (**Seeded Data**), the naming for the data seeded (**Naming**) and how to check that the data is created in Content Server (**Verify**).

Table 11–3 Group Spaces Seeded Data

Seeded Data	Naming	Verify
Security Group	One security group is seeded: <i>ApplicationName</i> For example: WC1	In Content Server, go to Administration > Admin Applets > User Admin > Security > Permission by Group
Roles	Two roles are seeded: <ul style="list-style-type: none"> ▪ <i>ApplicationName</i> User (with R permission on the security group) ▪ <i>ApplicationName</i> AuthenUser (with RWD permission on the security group) For example: WC1User and WC1AuthenUser	In Content Server, go to Administration > Admin Applets > User Admin > Security > Permission by Role
Root Folder name	<i>RootFolder</i> (with Security Group =<ApplicationName>) For example: /WebCenter1	Browse content (folder will be listed as a top-level folder)
Default Attributes - Public users	All public users have: <ul style="list-style-type: none"> ▪ Read on the account prefix PUBLIC ▪ Read on the account prefix WCILS ▪ The <i>ApplicationName</i>User role 	Query the <code>ExtendedConfigProperties</code> table, or after logging into Content Server, click on the username to view the user's profile page listing their roles and accounts, including the account PUBLIC and WCILS and the role <ApplicationName>User

Table 11-3 (Cont.) Group Spaces Seeded Data

Seeded Data	Naming	Verify
Default Attributes - Authenticated users	All Authenticated users have: <ul style="list-style-type: none"> ▪ Read permission on the account prefix AUTHEN ▪ Read, Write, Delete, Admin permission on the account prefix WCILS ▪ The <i>ApplicationNameAuthenUser</i> role 	Query the ExtendedConfigProperties table, or after logging into Content Server, click on the username to view the user's profile page listing their roles and accounts, including the account AUTHEN and WCILS and the role <i>ApplicationNameAuthenUser</i>
Workflows	Three workflows are seeded: <ul style="list-style-type: none"> ▪ <i>ApplicationNameAllApprover</i> ▪ <i>ApplicationNameAllReviewer</i> ▪ <i>ApplicationNameSingleApprover</i> For example, WC1AllApprover, WC1AllReviewer, and WC1SingleApprover	In Content Server, go to Administration > User Admin > Workflow Admin > Criteria tab

Personal Space data is seeded only once in a Content Server, regardless of how many Spaces instances are using the same Content Server. Therefore, if you have multiple Spaces instances using the same Content Server, they will all share the same Personal Spaces data.

Table 11-4 illustrates the Personal Space data that is seeded (**Seeded Data**), the naming for the data seeded (**Naming**) and how to check that the data is created in Content Server (**Verify**).

Table 11-4 Personal Space Seeded Data

Seeded Data	Naming	Verify
Security Group	One security group is seeded: PersonalSpaces	In Content Server, go to Administration > Admin Applets > User Admin > Security > Permission by Group
Roles	Two roles are seeded: <ul style="list-style-type: none"> ▪ PersonalSpacesRole (with R permission on the security group PersonalSpaces) ▪ PersonalSpacesAuthenRole (with RWD on the security group PersonalSpaces) 	In Content Server, go to Administration > Admin Applets > User Admin > Security > Permission by Role
Root Folder name	PersonalSpaces (with Security Group=PersonalSpaces)	Browse content (folder will be listed as a top-level folder)

Table 11–4 (Cont.) Personal Space Seeded Data

Seeded Data	Naming	Verify
Default Attributes - Public users	All public users have: <ul style="list-style-type: none"> ▪ Read on the Root Folder’s account ▪ The PersonalSpaces role 	Query the ExtendedConfigProperties table, or after logging into Content Server, click on the username to view the user’s profile page listing their roles and accounts, including the account PEWebCenter/PU and the role PersonalSpacesRole
Default Attributes - Authenticated users	All Authenticated users have: <ul style="list-style-type: none"> ▪ The PersonalSpacesAuthenRole role 	Query the ExtendedConfigProperties table, or after logging into Content Server, click on the username to view the user’s profile page listing their roles and accounts, including the role PersonalSpacesAuthenRole

11.3 Configuring Microsoft SharePoint Repositories

If you want to access a Microsoft SharePoint content repository from a WebCenter Portal application, you must install the Oracle WebCenter adapter for Microsoft SharePoint.

The Oracle WebCenter adapter for Microsoft SharePoint supports the following features:

- Reading content and metadata from the Microsoft SharePoint repository
- Writing files and folders to the SharePoint document libraries
- Running queries on the Microsoft SharePoint system
- Enabling SharePoint security settings for the accessed content by leveraging native Microsoft SharePoint authentication and authorization

All features are implemented using native Microsoft SharePoint web services as the interface to Microsoft SharePoint content and services.

This section discusses prerequisites for connecting WebCenter Portal applications to Microsoft SharePoint:

- [Section 11.3.1, "Microsoft SharePoint - Installation"](#)
- [Section 11.3.2, "Microsoft SharePoint - Configuration"](#)
- [Section 11.3.3, "Microsoft SharePoint - Security Considerations"](#)
- [Section 11.3.4, "Microsoft SharePoint - Limitations in WebCenter Portal"](#)
- [Section 11.3.5, "Managing Microsoft SharePoint Connections Using WLST"](#)

Note: To enable Microsoft SharePoint connections in Spaces, read the whitepaper "*Integrating the SharePoint 2007 Adapter with WebCenter Spaces*" available from Oracle Technology Network at <http://www.oracle.com/technetwork/middleware/webcenter/overview/index.html>.

11.3.1 Microsoft SharePoint - Installation

This section includes the following:

- [Section 11.3.1.1, "What You Should Know About Microsoft SharePoint Server Installation"](#)
- [Section 11.3.1.2, "Installing Oracle WebCenter Adapter for Microsoft SharePoint"](#)
- [Section 11.3.1.3, "Installing WLST Command Scripts for Managing Microsoft SharePoint Connections"](#)

11.3.1.1 What You Should Know About Microsoft SharePoint Server Installation

Oracle WebCenter Portal supports the following Microsoft SharePoint versions:

- Microsoft Office SharePoint Server (MOSS) 2007 SP2
- Microsoft Windows SharePoint Services (WSS) version 3 SP2

Note: A Microsoft SharePoint site configured for anonymous access is not supported by the adapter.

Refer to the appropriate Microsoft SharePoint documentation for installation information.

Oracle WebCenter Portal supports the following Microsoft SharePoint 2007 Document Library version settings:

- Require Check Out: No
- Content Approval: No
- Document Version History: No versioning

If any other version settings are configured, Oracle WebCenter adapter for Microsoft SharePoint does not function correctly. For example, if `Require CheckOut` is set to `yes`, upload operations fail. Similarly, if document version history or content approval is enabled, new versions or documents have restricted visibility.

11.3.1.2 Installing Oracle WebCenter Adapter for Microsoft SharePoint

The files for Oracle WebCenter adapter for Microsoft SharePoint are located in the Oracle WebCenter Companion DVD in the `ofm_wc_generic_jcr_sharepoint_adapter_11.1.1.4.0.zip` file. When you extract this ZIP file to a temporary location, you will find the adapter files in the `TEMP_LOCATION/WebCenter/services/content/adapters` directory.

Before You Begin:

WebCenter adapter for Microsoft SharePoint must be installed in the same managed server as your WebCenter Portal application. If you have not done so already, create a managed server suitable for WebCenter Portal application deployments as described

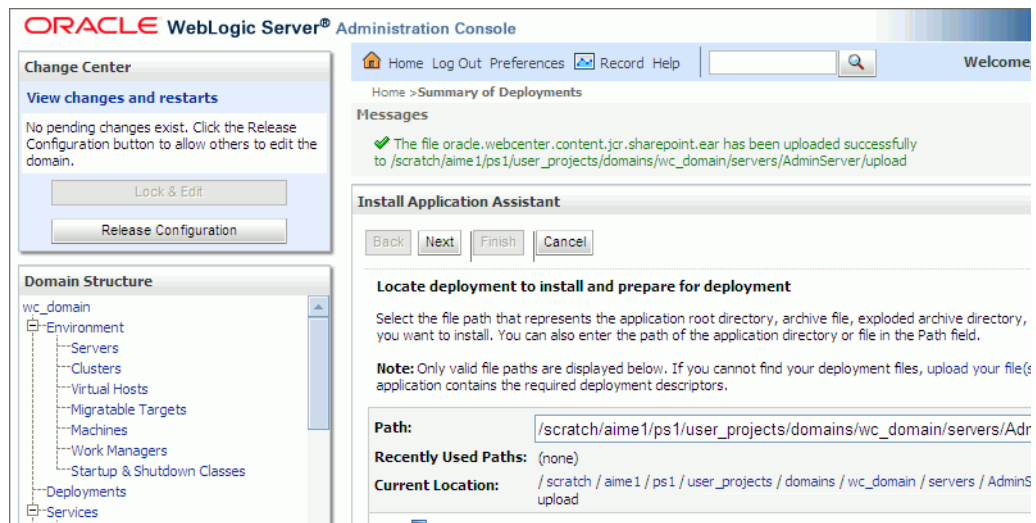
in [Section 7.1.4, "Creating a Managed Server"](#) and [Section 7.1.5, "Creating and Registering the Metadata Service Repository."](#)

To install WebCenter adapter for Microsoft SharePoint for a WebCenter Portal application:

1. Log in to the WLS Administration Console.

For information on logging into the WLS Administration Console, see [Section 1.13.2, "Oracle WebLogic Server Administration Console."](#)
2. Navigate to the WLS Administration Console's Home page.
3. From the **Domain Structure** pane, click **Deployments**.
4. In the **Summary of Deployments** section, under **Control**, click **Install**.
5. In **Install Application Assistant**, in **Note**, click the **upload your file(s)** link in the body of the text.
6. Click **Browse** next to **Deployment Archive**, select the `oracle.webcenter.content.jcr.sharepoint.ear` file from the `TEMP_LOCATION/WebCenter/services/content/adapters` directory. This is the temporary directory in which you extracted the contents of the `ofm_wc_generic_jcr_sharepoint_adapter_11.1.1.4.0.zip` file from the **Oracle WebCenter Companion DVD**. Click **Next**.
7. After you see the message that the EAR file has been uploaded successfully, as shown in [Figure 11–4](#), click **Next**.

Figure 11–4 Install Application Assistant



8. Select **Install this deployment as a library**, if not already selected, and click **Next**.
9. In **Select deployment targets**, select the managed server on which the WebCenter Portal: Framework application will be deployed. This must be a custom managed server (based on the Custom Portal template), not one of WebCenter Portal's out-of-the-box managed servers. For details, see the section "Using Templates to Create Custom Managed Servers" in *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Portal*.
10. Click **Next**.
11. In **Optional Settings**, accept the defaults and click **Finish**.

11.3.1.3 Installing WLST Command Scripts for Managing Microsoft SharePoint Connections

1. Extract the files `DocLibSharePointWLST.py` and `DocLibGenericWLST.py` from the `ofm_wc_generic_jcr_sharepoint_adapter_11.1.1.4.0.zip` file located in the Oracle WebCenter Companion DVD. These files are in the `/WebCenter/services/content/adapters` directory.
2. Copy the extracted `DocLibSharePointWLST.py` and `DocLibGenericWLST.py` files and paste them in the `ORACLE_HOME/common/wlst` directory.
3. To run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

For information about managing connections using WLST, see [Section 11.3.5, "Managing Microsoft SharePoint Connections Using WLST."](#)

11.3.2 Microsoft SharePoint - Configuration

You must perform the following tasks to enable Microsoft SharePoint connections in WebCenter Portal applications:

1. Install Oracle WebCenter adapter for Microsoft SharePoint in the same managed server where you plan to deploy your WebCenter Portal application.
2. In JDeveloper, configure a connection to your Microsoft SharePoint repository. This must be an application connection created in Application Resources in the Application Navigator.
3. (Optional) In JDeveloper, include a Documents task flow that uses the Microsoft SharePoint repository connection.
4. Deploy your WebCenter Portal application.

After deployment, you can access the Microsoft SharePoint repository that you configured in JDeveloper from your WebCenter Portal application.

5. (Optional) Reconfigure Microsoft SharePoint connection details postdeployment, if required.
 - a. Install WLST command scripts for managing Microsoft SharePoint connections postdeployment.
 - b. Modify the existing connection details (`setJCRSharePointConnection`) or create a new Microsoft SharePoint repository connection (`createJCRSharePointConnection`).

Note: To enable Microsoft SharePoint connections in Spaces, read the whitepaper "*Integrating the SharePoint 2007 Adapter with WebCenter Spaces*" available from Oracle Technology Network at <http://www.oracle.com/technetwork/middleware/webcenter/overview/index.html>.

11.3.3 Microsoft SharePoint - Security Considerations

Authentication through identity propagation is not supported on Microsoft SharePoint connections. However, you can use an external application to authenticate users against the Microsoft SharePoint repository. Use the WLST argument `extAppId` to specify the external application to use. For details, see [Section 11.3.5.1, "createJCRSharePointConnection."](#) Note that if the `extAppId` refers to an external application connection for which neither public nor shared credentials are defined,

then Documents task flows will prompt for credentials. This allows per-user mapping of credentials as an alternative to identity propagation.

11.3.4 Microsoft SharePoint - Limitations in WebCenter Portal

The Spaces application does not support Microsoft SharePoint as the primary document store, and therefore, you must use Oracle WebCenter Content instead.

11.3.5 Managing Microsoft SharePoint Connections Using WLST

Use the commands listed in [Table 11-5](#) to manage connections to SharePoint content repositories, postdeployment.

Configuration changes made using these WebCenter Portal WLST commands are only effective after you restart the Managed Server on which the WebCenter Portal application is deployed. For details, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

Table 11-5 SharePoint Content Repository WLST Commands

Use this command...	To...	Use with WLST...
createJCRSharePointConnection	Create a Microsoft SharePoint 2007 repository connection.	Online
setJCRSharePointConnection	Edit a Microsoft SharePoint 2007 repository connection.	Online
listJCRSharePointConnections	List all Microsoft SharePoint 2007 connections that are configured for a WebCenter Portal application.	Online

For information about how to install WLST scripts for Microsoft SharePoint, see [Section 11.3.1.3, "Installing WLST Command Scripts for Managing Microsoft SharePoint Connections."](#)

11.3.5.1 createJCRSharePointConnection

The `createJCRSharePointConnection` WLST command creates a connection to a Microsoft SharePoint 2007 repository. For syntax and other information about this WLST command, see "createJCRSharePointConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

Note: For WebCenter Portal applications, the `createJCRSharePointConnection` command works only if the application was developed to support Microsoft SharePoint connections in the first place. If the original WebCenter Portal application deployment does not include a Microsoft SharePoint connection, then the application will not contain the code necessary to support any new Microsoft SharePoint connections that you may want to create using this command. See also, [Section 11.3.2, "Microsoft SharePoint - Configuration."](#)

11.3.5.2 setJCRSharePointConnection

This WLST command edits an existing Microsoft SharePoint 2007 repository connection. For syntax and other information about this WLST command, see

"setJCRSharePointConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

11.3.5.3 listJCRSharePointConnections

This WLST command lists all of the SharePoint connections that are configured for a named WebCenter Portal application. For syntax and other information about this WLST command, see "listJCRSharePointConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

11.4 Configuring Oracle Portal Repositories

This section discusses the prerequisites for an Oracle Portal content repository in the following subsections:

- [Section 11.4.1, "Oracle Portal - Installation"](#)
- [Section 11.4.2, "Oracle Portal - Configuration"](#)
- [Section 11.4.3, "Oracle Portal - Security Considerations"](#)
- [Section 11.4.4, "Oracle Portal - Limitations in WebCenter Portal"](#)

11.4.1 Oracle Portal - Installation

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

11.4.2 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*.

11.4.3 Oracle Portal - Security Considerations

None.

11.4.4 Oracle Portal - Limitations in WebCenter Portal

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

You can expose Oracle Portal pages in WebCenter Portal applications 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 Portal:

- 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.

11.5 Configuring a File System Repository

This section discusses the prerequisites for a file system content repository in the following subsections:

- [Section 11.5.1, "File System - Security Considerations"](#)
- [Section 11.5.2, "File System - Limitations in WebCenter Portal"](#)

Caution: File system connections *must not* be used in production or enterprise application deployments. This feature is provided for development purposes only. Connections created through the file system adapter can be used during the development of WebCenter Portal applications using Oracle JDeveloper.

WebCenter Portal: Spaces applications do not support file system connections.

11.5.1 File System - Security Considerations

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

11.5.2 File System - Limitations in WebCenter Portal

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.

11.6 Registering Content Repositories

This section contains the following subsections:

- [Section 11.6.1, "What You Should Know About Registering Content Repositories for Spaces"](#)
- [Section 11.6.2, "Registering Content Repositories Using Fusion Middleware Control"](#)

- [Section 11.6.3, "Registering Content Repositories Using WLST"](#)

11.6.1 What You Should Know About Registering Content Repositories for Spaces

Consider the following when registering Content Server repositories for WebCenter Portal: Spaces:

- At start up, Spaces creates seed data (if it does not already exist) in the primary/active/default repository for Spaces.
- For Spaces, a Content Server repository connection must always be provided as a primary connection, even if another repository such as Microsoft SharePoint is made available.
- A user name with administrative rights for the Content Server instance is required (Content Administrator). This user will be used to create and maintain folders for Spaces content, security groups and roles, and manage content access rights. The default content administrator is `sysadmin`.

Administrative privileges are required for this connection so that operations can be performed on behalf of Spaces users.

- `Root Folder` and `Application Name` values:
 - For the active connection in Spaces, the `Root Folder` and `Application Name` values are used to create the seed data in the Spaces repository to enable storage of space-related data.

WARNING: You should never change the `Root Folder` or `Application Name` values separately; you should always change both. That is, if you change the `Root Folder` value after configuring and running Spaces, then you must also change the `Application Name` value, and vice versa. That is, you must change both values (`Root Folder` and `Application Name`) to unique values if the Spaces application already contains the seed data.

When you change these values, the existing seed data is not renamed in the Content Server repository. Instead, new seed data is created using the new values, when you start the application. Once the application is started, new Spaces data is created under the new `Root Folder` and existing data under the old `Root Folder` is no longer available. This means that the Documents service will now be disabled in Spaces where the Documents service was previously enabled, prior to changing the `Root Folder`.

Note: Although the `Root Folder` and `Application Name` values change, the old root content repository folder still appears in search results, like any other root folder in Content Server.

- The `Root Folder` value is used as the name for the root folder within the content repository under which all Spaces content is stored. For the `Root Folder` value, you must specify a content repository folder that does not yet exist. Use the format: `/foldername`. For example: `/MyWebCenterSpaces`. The `Root Folder` cannot be `/`, the root itself, and it must be unique across different WebCenter Portal applications. The folder specified is created for you when the WebCenter Portal application starts up. Invalid entries include: `/`, `/foldername/`, `/foldername/subfolder`.

- The `Application Name`, which identifies the Spaces application within this content repository, must have a unique value (for example: `MyWCS`). The name must be 14 characters or less, begin with an alphabetical character, followed by any combination of alphanumeric characters or the underscore character. The name specified here is also used to name document-related workflows, as follows: `<applicationName><WorkflowName>` and `<applicationName><WorkflowStepName>`. When naming workflows, only the first 14 characters of the `Application Name` are used.

The `Application Name` value is used for the following:

- * To separate data when multiple Spaces applications share the same content repository and should be unique across applications.
- * As the prefix to the seeded workflow and workflow steps.
- * As the name of the security group in which all data created in that Spaces application is stored.
- * As the prefix for the role (the name format is `applicationNameUser` and `applicationNameAuthenUser`).
- * To stripe users permissions on accounts for the particular Spaces application.
- * To stripe default attributes for the particular Spaces application.

For information about security groups and roles, see *Managing Security and User Access for Content Server*. For information about folders, see *Folders and WebDav Administration Guide*. These guides are available at http://download.oracle.com/docs/cd/E10316_01/owc.htm.

11.6.2 Registering Content Repositories Using Fusion Middleware Control

Follow the steps below to register a Content Server, Oracle Portal, or file system content repository using Fusion Middleware Control. Note that to register a SharePoint repository you must use WLST as described in [Section 11.6.3, "Registering Content Repositories Using WLST."](#) For information on how to register a Content Server repository using WLST, see [Section 11.10.2, "Setting Connection Properties for the Spaces Content Repository Using WLST."](#)

To register a Content Server, Oracle Portal, or file system content repository:

1. Log in to Fusion Middleware Control and navigate to the home page for the Spaces or Framework application:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:
 - For WebCenter Portal: Spaces - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For WebCenter Portal: Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > 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 11-5](#)).

Figure 11–5 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 11–6](#).

Table 11–6 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 Portal 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"> ▪ Content Server - an Oracle Universal Content Management repository. See Section 11.2, "Configuring Oracle WebCenter Content Server Repositories". ▪ Oracle Portal - an Oracle Portal content repository. See Section 11.4, "Configuring Oracle Portal Repositories." ▪ File System - a computer file system. See Section 11.5, "Configuring a File System Repository." <p>Caution: 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>(Spaces) If you are setting up the back-end content repository for Spaces, that is, the repository used by Spaces to store space-related documents, you must select Content Server.</p>

Table 11–6 (Cont.) Manage Content Repository Connections

Field	Description
Active Connection	<p>Select to make this the <i>default</i> or <i>primary</i> content repository for your WebCenter Portal application.</p> <p>You can connect your WebCenter Portal 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 data-bbox="683 443 1377 705">■ For the Spaces application: Select to make this the <i>active connection</i>, that is, the back-end repository that Spaces uses to store space-related documents. The active connection must be to an Content Server. If this is the <i>active connection</i> for Spaces, some additional configuration is required -- see Section 11.6.1, "What You Should Know About Registering Content Repositories for Spaces." <li data-bbox="683 722 1377 915">■ For Framework applications: Select to make this the <i>active connection</i>; that is, the default connection for Content Presenter, Document Manager, Document List Viewer, and Recent Documents task flows. When no specific connection details are provided for these task flows, this default (also called <i>primary, active</i>) connection is used. <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 Spaces only.) Enter additional details for the Spaces repository. For information, see [Section 11.6.1, "What You Should Know About Registering Content Repositories for Spaces."](#)
7. Enter connection details for the content repository. For detailed parameter information, see:
 - [Table 11–7, "Content Server Connection Parameters"](#)
 - [Table 11–8, "Connection - Content Server - Cache Details"](#)
 - [Table 11–9, "Oracle Portal Connection Parameters"](#)
 - [Table 11–10, "File System Connection Parameters"](#)

Table 11-7 Content Server Connection Parameters

Field	Description
RIDC Socket Type	<p>Specify whether 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"> ▪ Socket - Uses an <code>intradoc</code> socket connection to connect to the Content Server. The client IP address must be added to the list of authorized addresses in Content Server. In this case, the client is the machine on which Oracle WebCenter Portal is running. ▪ Socket SSL - Uses an <code>intradoc</code> socket connection to connect to 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 Spaces). ▪ Web - Uses an HTTP(S) connection to connect to Content Server. ▪ JAX-WS - Uses an HTTP(S) connection to connect to Content Server. <p>For Spaces, the Web option is not suitable for the active connection, that is, the back-end Content Server repository that is being used to store space-related documents because it does not allow identity propagation.</p>
Server Host	<p>Enter the host name of the machine where Content Server is running. For example: <code>mycontentserver.mycompany.com</code></p> <p>Server Host is required when the RIDC Socket Type is set to Socket or Socket SSL.</p>
Server Port	<p>Enter the port on which the Content Server listens:</p> <ul style="list-style-type: none"> ▪ Socket - Port specified for the <code>incoming</code> provider in the server. ▪ Socket SSL - Port specified for the <code>sslincoming</code> provider in the server. <p>This property corresponds to the <code>IntradocServerPort</code> setting in the Content Server configuration file, which defaults to port 4444.</p> <p>Server Port is required when the RIDC Socket Type is set to Socket or Socket SSL.</p>
Web URL	<p>Enter the Web server URL for the Content Server.</p> <p>Use the format: <code>http://hostname:portnumber/web_root/plugin_root</code></p> <p>For example: <code>http://mycontentserver/cms/idcplg</code></p> <p>Web URL is applicable when the RIDC Socket Type is set to Web.</p>
Web Service URL	<p>Enter the Web service URL required to connect to Content Server when using the JAX-WS protocol.</p> <p>Use the format: <code>http://hostname:port/web_root</code></p> <p>For example: <code>http://myhost.com:9044/idcnativews</code></p> <p>Web Service URL is applicable when RIDC Socket Type is set to JAX-WS.</p>
Connection Timeout (ms)	<p>Specify the length of time allowed to log in to Content Server (in milliseconds) before issuing a connection timeout message. If no timeout is set, there is no time limit for the login operation.</p>

Table 11-7 (Cont.) Content Server Connection Parameters

Field	Description
Authentication Method	<p>Choose from:</p> <ul style="list-style-type: none"> <li data-bbox="630 302 1380 449">■ Identity Propagation - Content Server and the WebCenter Portal application use the same identity store to authenticate users. (Spaces) Identity propagation is required on the active connection for Spaces, that is, for the content repository being used to store space-related documents. <li data-bbox="630 462 1380 592">■ External Application - An external application authenticates users against the Content Server. Select this option if you want to use public, shared, or mapped credentials. See also, "Setting Security for the Documents Service" in the <i>Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal</i>. <p>If an external application is used for authentication, use the Associated External Application drop down list to identify the application. If the application you want is not listed, select Create New to define the external application now.</p>

Table 11-7 (Cont.) Content Server Connection Parameters

Field	Description
Web Server Context Root	<p>Enter the Web server context root for Content Server. Use the format /<context_root>. For example, /cs.</p> <p>When specified, several Content Server features based on iFrame are available in the WebCenter Portal application. This includes:</p> <ul style="list-style-type: none"> ▪ Associating a content profile with files when uploading new or updated files to Content Server. For more information, see "Uploading New Files" and "Uploading a New Version of an Existing File" in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces</i>. ▪ Using the document review functionality available in Oracle AutoVue. For more information, see "Reviewing and Collaborating on Documents Using AutoVue" in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces</i>. ▪ Editing advanced document properties. For more information, see "Working with File Properties" in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces</i>. ▪ Viewing folder and file workflow details. For more information, see "Viewing Workflow Assignments" in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces</i>. ▪ Previewing files in a slide viewer. For more information, see "Opening a File" in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces</i>. ▪ Site Studio integration Without OHS (and WebContextRoot configuration), it is still possible to create or edit Site Studio content from within Content Presenter, but the create and edit actions launch new browser windows (or tabs) rather than opening within the Content Presenter task flow. For more information, see "Using Content Presenter to Create or Edit Oracle Site Studio Content" in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces</i>. <p>The Web Server Context Root property is only applicable when the Authentication Method is set to Identity Propagation.</p> <p>Note: Specifying the Web Server Context Root is an indicator that the WebCenter Portal application is front-ended by OHS. If you specify the Web Server Context Root and do not connect through OHS, a 404 error occurs while you attempt to edit the advanced metadata in the Document Viewer, upload using a profile, or click Details for a content item in a workflow in a space. For information about setting up OHS to front-end WebCenter Portal applications, see Appendix B, "Oracle HTTP Server Configuration for WebCenter Portal".</p> <p>If your WebCenter Portal application is connected to multiple Content Server servers, Oracle recommends that each Content Server server has a unique Web Server Context Root so that OHS re-direction works correctly.</p>
Associated External Application	<p>Select the external application used to authenticate users against Content Server.</p> <p>Associated External Application is applicable when RIDC Socket Type is set to Web and also when the RIDC Socket Type is Socket or Socket SSL (with Authentication Method set to External Application).</p>

Table 11–7 (Cont.) Content Server Connection Parameters

Field	Description
Client Security Policy	<p>Enter the client security policy to be used when the RIDC Socket Type is JAX-WS. For example: <code>oracle/wss11_saml_token_with_message_protection_service_policy</code></p> <p>The JAX-WS client security policy can be any valid OWSM policy, but must match the security policy configured for the Content Server's Native Web Services IdcWebLogin service. For more information about the IdcWebLogin service, see "WebCenter Content Web Services" in the <i>Oracle WebCenter Content Developer's Guide for Content Server</i>.</p> <p>Leave this field blank if your environment supports Global Policy Attachments (GPA).</p>
Administrator User Name	<p>Enter a user name with administrative rights for this Content Server instance. This user will be used to fetch content type information based on profiles and track document changes for cache invalidation purpose.</p> <p>Defaults to <code>sysadmin</code>.</p>
Administrator Password	<p>Enter the password for the Content Server administrator.</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 RIDC Socket 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 RIDC Socket 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 RIDC Socket 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 RIDC Socket Type is set to Socket SSL.</p>

Table 11–8 Connection - Content Server - Cache Details

Element	Description
Cache Invalidation Interval (minutes)	<p>Specify the frequency between checks for external Content Server content changes (in minutes). WebCenter Portal automatically clears items that have changed from the cache.</p> <p>The default is 0 which means that cache invalidation is disabled.</p> <p>The <i>minimum</i> interval is 2 minutes.</p>

Table 11–8 (Cont.) Connection - Content Server - Cache Details

Element	Description
Maximum Cached Document Size (bytes)	<p>Enter a maximum cacheable size (in bytes) for Content Server binary documents. Documents larger than this size are not cached by WebCenter Portal.</p> <p>The default is 102400 bytes (100K).</p> <p>Tune this value based on your machine's memory configuration and the types of binary documents that you expect to cache.</p>

Table 11–9 Oracle Portal Connection Parameters

Field	Description
Data Source Name	<p>Enter the JNDI DataSource location used to connect to the portal.</p> <p>For example: jdbc/MyPortalDS</p> <p>The datasource must be on the server where the WebCenter Portal application is deployed.</p>
Connection Timeout (ms)	<p>Specify the length of time allowed to log in to Oracle Portal (in milliseconds) before issuing a connection timeout message. If no timeout is set, there is no time limit for the login operation.</p>
Authentication Method	<p>Specify how to authenticate users against Oracle Portal. Choose from:</p> <ul style="list-style-type: none"> ▪ Identity Propagation - Select this option when the WebCenter Portal application and Oracle Portal both use the same user identity store. ▪ External Application - Use an external application to authenticate users against Oracle Portal. Select this option if you want to use public, shared, or mapped credentials. <p>If an external application is used for authentication, use the Associated External Application dropdown 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 dropdown list, or click Create New to configure a new external application now.</p>

Table 11–10 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>Caution: 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. Click **Test** to verify if the connection you created works. For a successful connection, the Test Status message displays the advice that to start using the new (active) connection, you must restart the managed server on which the WebCenter Portal application is deployed.

The registered connections are now available to Documents service and Content Presenter task flows, which you can add to pages in WebCenter Portal: Spaces or WebCenter Portal: Framework applications. See also, "Working with the Documents Service Task Flows and Document Components" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

11.6.3 Registering Content Repositories Using WLST

Use the following WLST commands to register new content repository connections for Framework applications. For information on how to register a Content Server repository for Spaces using WLST, see [Section 11.10.2, "Setting Connection Properties for the Spaces Content Repository Using WLST."](#)

- **Content Server** - `createJCRContentServerConnection`
- **File System** - `createJCRFileSystemConnection`
- **Oracle Portal** - `createJCRPortalConnection`
- **Microsoft SharePoint** - [createJCRSharePointConnection](#)

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='1'`. See [Section 11.7, "Changing the Active \(or Default\) Content Repository Connection"](#).

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands"](#).

Note: To start using the new (active) connection you must restart the managed server on which the Framework application is deployed. See "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

11.7 Changing the Active (or Default) Content Repository Connection

WebCenter Portal applications support multiple content repository connections but only one content repository connection can be designated the active (or default) connection.

In Spaces, the *active connection* becomes the default back-end repository for space and Home space documents and the repository must be Content Server. The *active connection* is also used as the default connection for the Documents service and Content Presenter task flows.

For other WebCenter Portal applications, the *active connection* becomes the default connection for Content Presenter, Document Manager, Document List Viewer, and Recent Documents, and so on. When no specific connection details are provided for these task flows, the default (active) connection is used.

This section contains the following subsections:

- [Section 11.7.1, "Changing the Active \(or Default\) Content Repository Connection Using Fusion Middleware Control"](#)
- [Section 11.7.2, "Changing the Active \(or Default\) Content Repository Connection Using WLST"](#)

11.7.1 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 Portal: Spaces or the WebCenter Portal: Framework application:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:
 - For WebCenter Portal: Spaces - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For WebCenter Portal: Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
3. From the list of services on the WebCenter Portal 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** checkbox.
6. Click **OK** to update the connection.
7. Click **Test** to verify if the connection you activated works. For a successfully activated connection, the Test Status message displays the advice that to start using the updated connection you must restart the managed server on which the WebCenter Portal application is deployed.

11.7.2 Changing the Active (or Default) Content Repository Connection Using WLST

Use the following WLST commands with `isPrimary='1'` to designate an existing content repository connection as the default connection:

- **Content Server** - `setJCRContentServerConnection`
- **File System** - `setJCRFileSystemConnection`
- **Oracle Portal** - `setJCRPortalConnection`
- **Microsoft SharePoint** - [setJCRSharePointConnection](#)

See also, [listJCRSharePointConnections](#)

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 1.13.3.1, "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 Portal application is deployed. See, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

11.8 Modifying Content Repository Connection Details

This section contains the following subsections:

- [Section 11.8.1, "Modifying Content Repository Connection Details Using Fusion Middleware Control"](#)
- [Section 11.8.2, "Modifying Content Repository Connection Details Using WLST"](#)
- [Section 11.8.3, "Modifying Cache Settings for Content Presenter"](#)

11.8.1 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 Portal: Spaces or the WebCenter Portal: Framework application:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
3. From the list of services on the WebCenter Portal 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 11-7, "Content Server Connection Parameters"](#)
 - [Table 11-9, "Oracle Portal Connection Parameters"](#)
 - [Table 11-10, "File System Connection Parameters"](#)
6. Click **OK** to save your changes.
7. Click **Test** to verify if the updated connection works. For a successfully updated connection, the Test Status message displays the advice that to start using the updated connection, you must restart the managed server on which the WebCenter Portal application is deployed.

11.8.2 Modifying Content Repository Connection Details Using WLST

Use the following WLST commands to edit content repository connections:

- **Oracle WebCenter 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='1'`. See [Section 11.7, "Changing the Active \(or Default\) Content Repository Connection"](#).

For information on how to run WLST commands, see [Section 1.13.3.1, "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 Portal application is deployed. See "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

11.8.3 Modifying Cache Settings for Content Presenter

The content management code for Content Presenter, the Content Management Interoperability Services (CMIS) REST APIs, and so on, are shipped out of the box with local (in-memory) caches. This code doesn't use Coherence by default, although Coherence is the recommended caching mechanism for production and a requirement for HA environments. You can enable Coherence for caches in the `content-coherence-cache-config.xml` file. For WebCenter Portal: Spaces this file is stored in the

`ORACLE_HOME/user_projects/applications/wc_domain/custom.webcenter.spaces.fwk/APP-INF/classes/` directory. For WebCenter Portal applications, developers must create the `content-coherence-cache-config.xml` file in the application (EAR) classpath or server's system classpath.

A sample Coherence configuration file, as shown in [Example 11-1](#), is provided within the `content-app-lib.ear` file. This EAR file is located at: `ORACLE_HOME/webcenter/modules/oracle.webcenter.content.integration_11.1.1/content-app-lib.ear`. The sample file location is: `/content-app-lib.ear/APP-INF/classes/sample-content-coherence-cache-config.xml` file. You can copy this file and rename it to `content-coherence-cache-config.xml`, and then set the values to meet customer's deployment needs. [Table 11-11](#) describes the cache entries in this file.

Example 11-1 Sample Coherence Configuration File

```
<!DOCTYPE cache-config SYSTEM "cache-config.dtd">
<cache-config>
  <caching-scheme-mapping>
    <cache-mapping>
      <cache-name>repo.ucm.nodeUidCache.*</cache-name>
      <scheme-name>ContentNodeCaches</scheme-name>
    </cache-mapping>
    <cache-mapping>
      <cache-name>repo.ucm.nodePathToUidCache.*</cache-name>
      <scheme-name>ContentNodeCaches</scheme-name>
    </cache-mapping>
    <cache-mapping>
      <cache-name>repo.ucm.securityInfoCache.*</cache-name>
```

```

        <scheme-name>ContentNodeCaches</scheme-name>
    </cache-mapping>
<cache-mapping>
    <cache-name>repo.ucm.typeNameCache.*</cache-name>
    <scheme-name>ContentTypeCaches</scheme-name>
</cache-mapping>
<cache-mapping>
    <cache-name>repo.ucm.typeNamesCache.*</cache-name>
    <scheme-name>ContentTypeCaches</scheme-name>
</cache-mapping>
<cache-mapping>
    <cache-name>binaryCache.*</cache-name>
    <scheme-name>ContentBinaryCaches</scheme-name>
</cache-mapping>
<cache-mapping>
    <cache-name>repo.ucm.searchCriteriaCache.*</cache-name>
    <scheme-name>ContentSearchCaches</scheme-name>
</cache-mapping>
<cache-mapping>
    <cache-name> repo.ucm.indexedFieldsCache.*</cache-name>
    <scheme-name>ContentSearchCaches</scheme-name>
</cache-mapping>
<cache-mapping>
    <cache-name>repo.ucm.securityUserCache.*</cache-name>
    <scheme-name>ContentSecurityCaches</scheme-name>
</cache-mapping>
<cache-mapping>
    <cache-name>repo.ucm.profileTriggerValueCache.*</cache-name>
    <scheme-name>ContentProfileCaches</scheme-name>
</cache-mapping>
</caching-scheme-mapping>
<caching-schemes>
<!--
    The following schemes are all local. For a clustered deployment,
    a distributed, replicated, or other clustered scheme is recommended.
    See Coherence documentation for more information.
-->
<local-scheme>
    <scheme-name>ContentNodeCaches</scheme-name>
    <expiry-delay>1m</expiry-delay>
    <high-units>100</high-units>
</local-scheme>
<local-scheme>
    <scheme-name>ContentTypeCaches</scheme-name>
    <expiry-delay>30m</expiry-delay>
    <high-units>50</high-units>
</local-scheme>
<local-scheme>
    <scheme-name>ContentBinaryCaches</scheme-name>
    <expiry-delay>1m</expiry-delay>
    <high-units>100000</high-units>
    <unit-calculator>
        <class-scheme>
            <class-name>com.tangosol.net.cache.SimpleMemoryCalculator</class-name>
        </class-scheme>
    </unit-calculator>
</local-scheme>
<local-scheme>
    <scheme-name>ContentSearchCaches</scheme-name>
    <expiry-delay>5m</expiry-delay>

```

```

        <high-units>50</high-units>
    </local-scheme>
</local-scheme>
    <local-scheme>
        <scheme-name>ContentSecurityCaches</scheme-name>
        <expiry-delay>10m</expiry-delay>
        <high-units>50</high-units>
    </local-scheme>
</local-scheme>
    <local-scheme>
        <scheme-name>ContentProfileCaches</scheme-name>
        <expiry-delay>1h</expiry-delay>
        <high-units>100</high-units>
    </local-scheme>
</local-scheme>
    <!--
<class-scheme>
    <scheme-name>ContentDisabledCaches</scheme-name>
    <class-name>com.tangosol.util.NullImplementation$NullMap</class-name>
</class-scheme>
-->
</caching-schemes>
</cache-config>
    
```

Table 11–11 Cache Entries in content-coherence-cache-config.xml

Cache Entry Name	Description
repo.ucm.nodeUidCache.*	<p>Stores a list of nodes for a repository based on an ID. The size of this cache entry depends upon the number of nodes in the active repository.</p> <p>This cache expires based on when the node data is refreshed and how many times the data is modified from another application.</p> <p>Key - Node UID - String</p> <p>Value - A Content Server Node object</p>
repo.ucm.nodePathToUidCache.*	<p>Stores a list of nodes for a repository based on a path. The size of this cache depends upon the number of nodes in the active repository.</p> <p>This cache entry expires based on when the node data is refreshed and how many times the data is modified from another application. The size and expiration time must be the same as that of nodeUidCache.</p> <p>Key - Node path - String</p> <p>Value - Node UID - String</p>
repo.ucm.securityInfoCache.*	<p>Stores cached security information for a node. The size of this cache depends upon the number of nodes in the repository. This cache expires based on the frequency of node security data updates.</p> <p>Key - Node UID - String</p> <p>Value - Security information for a node</p>
repo.ucm.typeNameCache.*	<p>Caches Content Type information. The size of this cache depends upon the number of types in the repository. This cache expires based on when the type information is refreshed and how many times the types are modified from another application.</p> <p>Key - Content Type UID - String</p> <p>Value - A ContentType object</p>

Table 11-11 (Cont.) Cache Entries in content-coherence-cache-config.xml

Cache Entry Name	Description
repo.ucm.typeNamesCache.*	<p>Caches all the type names known to Content Server. All type names are cached together (one key), and thus all expire at the same time.</p> <p>This cache expires based on the frequency of new types being created or removed.</p> <p>Key - There is only one key to this cache: "typeNames"</p> <p>Value - An ArrayList<String> of the type names</p>
binaryCache.*	<p>Caches binary property data. Only binaries that are smaller than the repository configuration property BinaryCacheMaxEntrySize are cached.</p> <p>The size of this cache either depends on the number and frequency of the smaller binary properties (smaller than the BinaryCacheMaxEntrySize setting) usage, or it is based on the total amount of memory to be used for binary caches.</p> <p>This cache expires based on when the binary data is refreshed and how many times this data is modified from another application.</p> <p>Key - The Node UID and binary Property UID (nodeUid.propUid) - String</p> <p>Value - The binary stream data - byte[]</p>
repo.ucm.searchCriteriaCache.*	<p>Caches a set of search query to parameters based on the Content Server search grammar. The size of this cache depends upon the number of unique searches expected to be repeatedly performed.</p> <p>The expiration must be set to eventually expire unused searches and save on the cache memory.</p> <p>Key - A set of search query parameters.</p> <p>Value - A set of search query parameters, in Content Server terms.</p>
repo.ucm.indexedFieldsCache.*	<p>Holds the indexed (searchable) system properties for the repository. There are three keys in this cache:</p> <ul style="list-style-type: none"> ▪ "indexedFields" holds all Content Server indexed fields. ▪ "indexedFolderProps" holds indexed system properties for folders. ▪ "indexedDocProps" holds indexed system properties for documents. <p>This cache expires based on the frequency of the indexed fields changes.</p> <p>Key - String</p> <p>Value - Map<String, Boolean> holds a key for each indexed property name, and a boolean indicating if that property is also sortable.</p>
repo.ucm.securityUserCache.*	<p>Caches the mapping between local user names (current application) and the name of the same user in Content Server. The size of this cache depends upon the number of simultaneous and/or frequent users.</p> <p>This cache expires based on the frequency of user identity mapping updates.</p> <p>Key - Local user Id - String</p> <p>Value - Content Server user Id - String</p>

Table 11–11 (Cont.) Cache Entries in content-coherence-cache-config.xml

Cache Entry Name	Description
repo.ucm.profileTriggerValueCache.*	<p>Caches the profile trigger value for a given profile, so it is available when documents are created. The maximum number of entries in this cache is implicitly limited to the maximum number of profiles on the Content Server server. The cache entry size is small. The primary entry to vary is the expiration, which depends upon how often the profile trigger field values are modified in Content Server. These values change rarely once a profile is configured on the Content Server system. Therefore, the expiration should be set appropriately.</p> <p>Key - The Content Server profile name - String</p> <p>Value - The Content Server profile trigger value - String</p>

11.9 Deleting Content Repository Connections

This section contains the following subsections:

- [Section 11.9.1, "Deleting Content Repository Connections Using Fusion Middleware Control"](#)
- [Section 11.9.2, "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.

11.9.1 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 Portal: Spaces or the WebCenter Portal: Framework application:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
3. From the list of services on the WebCenter Portal 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 Portal application is deployed.

11.9.2 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 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands"](#).

Note: To effect this change you must restart the managed server on which the WebCenter Portal application is deployed. See, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

11.10 Setting Connection Properties for the Spaces Content Repository

You can view, modify, and delete connection properties for the back-end Content Server repository that is being used by Spaces to store space and Home space documents. Specifically, you can define the root folder under which space content is stored, the name of the content repository administrator, and a unique application identifier for separating application data on Content Server.

This section contains the following subsections:

- [Section 11.10.1, "Setting Connection Properties for the Spaces Content Repository Using Fusion Middleware Control"](#)
- [Section 11.10.2, "Setting Connection Properties for the Spaces Content Repository Using WLST"](#)

11.10.1 Setting Connection Properties for the Spaces Content Repository Using Fusion Middleware Control

To set content repository connection properties for Spaces:

1. Log in to Fusion Middleware Control and navigate to the home page for the Spaces application. See [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#).
2. From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
3. From the list of services on the WebCenter Portal Services Configuration page, choose **Content Repository**.
4. Select the connection name, and click **Edit**.
5. (For the active connection in Spaces only.) Set connection properties for the Spaces repository. For information, see [Section 11.6.1, "What You Should Know About Registering Content Repositories for Spaces."](#)
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 Spaces application is deployed.

11.10.2 Setting Connection Properties for the Spaces Content Repository Using WLST

The following commands are valid only for the Spaces application to view, set, and delete properties for the Content Server repository that is being used by Spaces to store space and Home 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 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

11.11 Testing Content Repository Connections

After setting up content repository connections, you can test them to make sure that you can access the content repository, as described in the following sections:

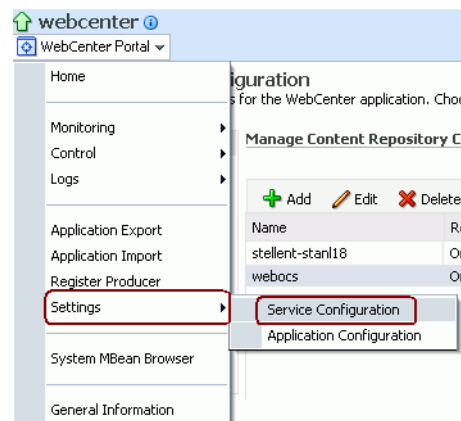
- [Section 11.11.1, "Testing Content Server Connections"](#)
- [Section 11.11.2, "Testing Oracle Portal Connections"](#)

11.11.1 Testing Content Server Connections

To verify a connection of the socket type web, log in to the Web interface of Content Server as administrator. You can obtain the URL of a socket type connection through Fusion Middleware Control as follows:

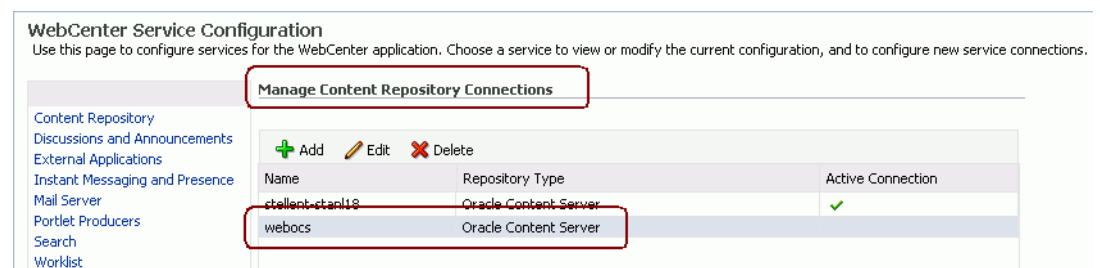
1. In Fusion Middleware Control, from the **WebCenter Portal** menu, choose **Settings** and select **Service Configuration** (Figure 11–6).

Figure 11–6 Fusion Middleware Control WebCenter Portal Menu



2. On the **Manage Content Repository Connections** page, select the connection and click **Edit** (Figure 11–7).

Figure 11–7 Manage Content Repository Connections Page



3. On the **Edit Content Repository Connection** page, copy the Web URL (Figure 11–8).

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 11–8 Edit Content Repository Connection Page

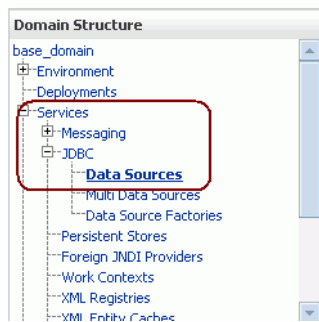


11.11.2 Testing Oracle Portal Connections

To verify the full state of an Oracle Portal connection:

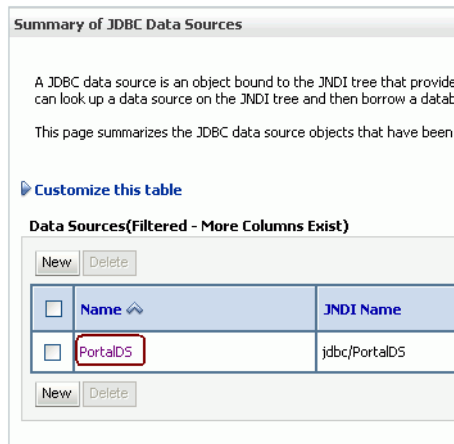
1. In the Oracle WebLogic Administration Console, under **Domain Structure**, expand **Services > JDBC**, then double-click **Data Sources** (Figure 11–9).

Figure 11–9 Oracle WebLogic Administration Console



2. On the **Summary of JDBC Data Sources** page, select the data source you intend to test (Figure 11–10).

Figure 11–10 Summary of JDBC Data Sources Page



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 11-11).

Figure 11-11 Data Source Settings Section



11.12 Changing the Maximum File Upload Size

By default, the maximum upload size for files is:

- 2 MB for WebCenter Portal: Framework applications. This default is imposed by Apache MyFaces Trinidad, which handles uploading files from a browser to the application server.

Framework application developers can customize the maximum file upload size at design time by setting the

`org.apache.myfaces.trinidad.UPLOAD_MAX_DISK_SPACE` parameter in the `web.xml` file. For more information, see "Setting Parameters to Upload Files to Content Repositories" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

If you want to change the maximum upload file size postdeployment, you must edit the `web.xml` file. For details, see [Section A.1.2.2, "Editing web.xml Properties for WebCenter Portal Applications."](#)

- 2 MB for Spaces applications.

System administrators can customize the maximum file upload size by editing the `uploadedFileMaxDiskSpace` parameter in the `webcenter-config.xml` file. For details, see [Section A.1.3, "webcenter-config.xml."](#)

Managing the Activity Graph Service

This chapter describes how to configure and manage the Activity Graph service for Oracle WebCenter Portal applications.

Always use the Activity Graph Administration, Fusion Middleware Control or WLST command-line tool to review and configure the Activity Graph service. Oracle does not recommend that you edit files manually (unless specifically instructed to do so) as this can lead to misconfiguration.

This chapter includes the following sections:

- [Section 12.1, "What You Should Know About the Activity Graph Service"](#)
- [Section 12.2, "Configuration Roadmaps for the Activity Graph Service"](#)
- [Section 12.3, "Activity Graph Service Prerequisites"](#)
- [Section 12.4, "Preparing Data for the Activity Graph Service"](#)
- [Section 12.5, "Customizing Reason Strings for Similarity Calculations"](#)
- [Section 12.6, "Managing Activity Graph Schema Customizations"](#)
- [Section 12.7, "Setting Up Activity Rank for Oracle Secure Enterprise Search"](#)
- [Section 12.8, "Troubleshooting Issues with Recommendations"](#)

Audience

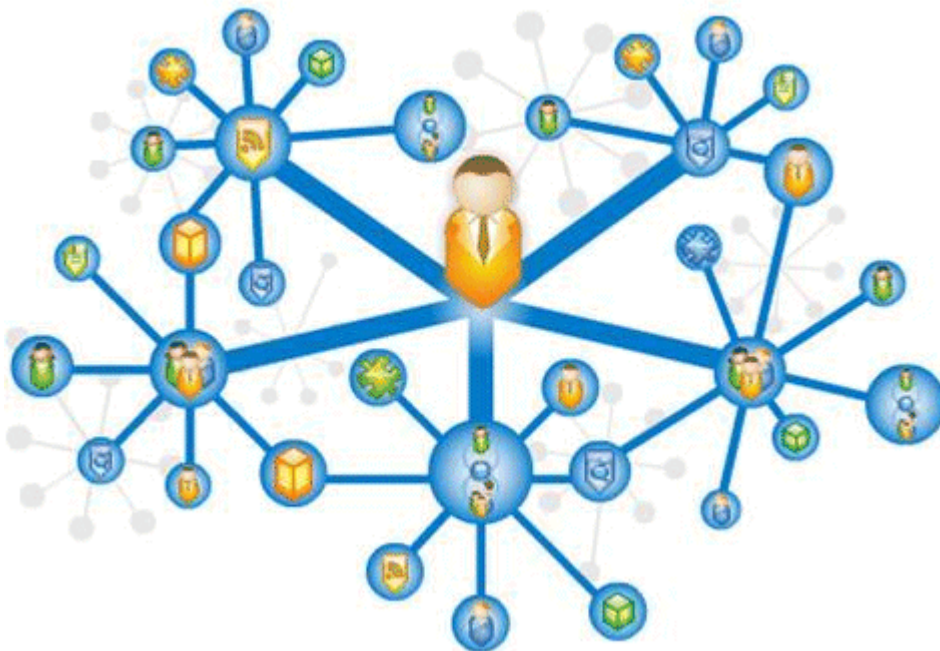
The content of this chapter is intended for Fusion Middleware administrators (users granted `Admin` or `Operator` role through the Oracle WebLogic Server Administration Console). See also, [Section 1.8, "Understanding Administrative Operations, Roles, and Tools."](#)

12.1 What You Should Know About the Activity Graph Service

The Activity Graph service provides suggestions of people that a user may be interested in connecting with, based on existing connections and shared interaction with objects in the application. It also directs users to spaces or content that may be of interest, based on similar interactions with those spaces or items that the user is currently viewing.

The Activity Graph service presents these suggestions based on data gathered and analyzed by the Activity Graph engines. The Activity Graph engines provide a central repository for actions that are collected by enterprise applications. Thinking in terms of a mathematical graph, application users and the enterprise content with which they interact are *nodes*, and the actions between users and between users and content are *directed edges* ([Figure 12-1](#)).

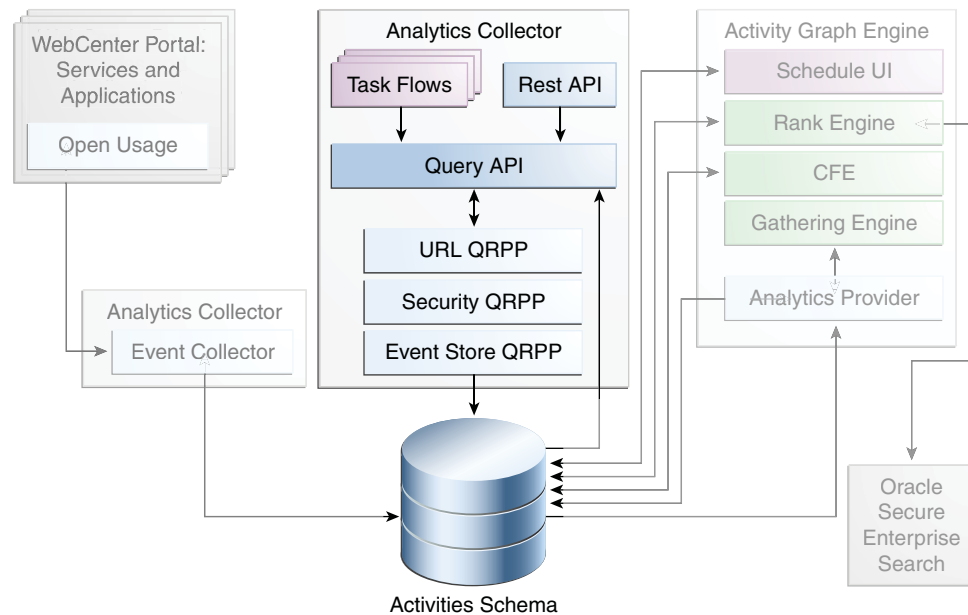
Figure 12–1 An Activity Graph



There are three main components used by the Activity Graph service:

- The Oracle Analytics Event Collector collects event data using the OpenUsage API and saves that data in the Activities database.
- The Activity Graph engines include engines for gathering data, calculating similarity scores, and calculating search rankings.
- The Activity Graph Query API exposes raw action data and processed recommendation data, and mechanisms (QRPPs) through which to filter results from people who do not have access to see them and decorate results with up-to-date metadata.

Figure 12–2 shows how the different components work together. The process is described below.

Figure 12–2 Activity Graph Service Architecture

When an action occurs in WebCenter Portal, for example, Monty viewing his document, it is picked up by the Analytics Events Collector and placed in an event table in the Activities database.

When the activity data gathering process starts, the Analytics Activity Provider reads actions from the Analytics event tables and uses a registered set of mappings to generate activities. An *activity* is one occurrence of an action and is used to determine *relations*, aggregated occurrences of actions, which are stored in the relation tables. For example, the fact that Monty has viewed this particular document five times is a relation. Information in the relation tables is used to determine recommendations and search ranks.

The Activity Graph Query API is a Java API, used by the Activity Graph service task flows, that queries the relation tables for recommendations using a recipe. A *recipe* is a weighted list of similarity calculations. A *similarity calculation* provides a similarity score (a number between zero and one) that designates how similar two objects are to each other given a specific criterion. The weighting of each calculation determines its significance in deciding the overall recommendation score. Recommendations are ordered by their total recommendation score. WebCenter Portal provides default similarity calculations, used by the Activity Graph service task flows. You can edit these similarity calculations or create custom similarity calculations. For more information, see the section "Defining Custom Similarity Calculations" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

After the initial list of recommendations for a particular object is generated, the results can be filtered into something more appropriate and useful to present to users. This is achieved using Query Result Post-Processors (QRPPs). QRPPs take the current list of recommendation results return a modified list as output. A QRPP may filter out recommendations, for example by removing recommendations for objects that the current user is not permitted to see, or may add or modify result metadata.

Recommendations are then presented to users via the Activity Graph service task flows. For more information, see the section "Activity Graph Service Task Flows" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

12.2 Configuration Roadmaps for the Activity Graph Service

Use the roadmaps in this section as an administrator’s guide through the configuration process:

- **Roadmap - Configuring the Activity Graph Service for the Spaces application**

The flow chart (Figure 12–3) and table (Table 12–1) in this section provide an overview of the prerequisites and tasks required to get the Activity Graph service working in the Spaces application.

Figure 12–3 Configuring the Activity Graph Service for the Spaces Application

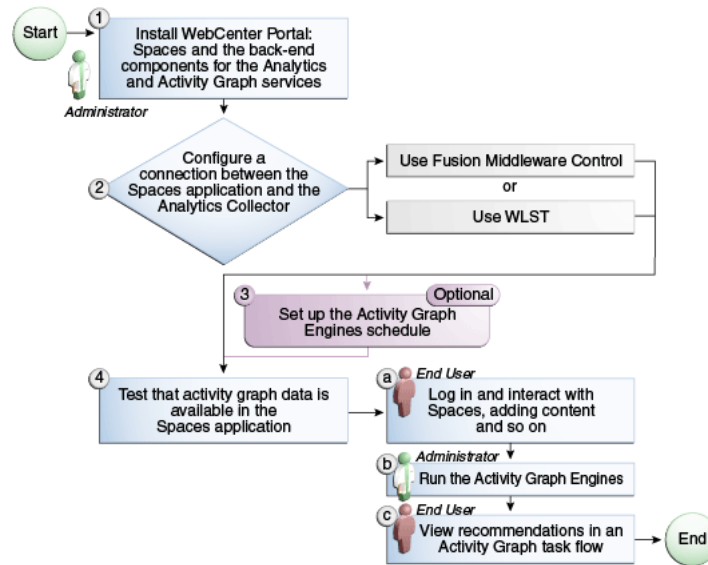


Table 12–1 Configuring the Activity Graph Service for the Spaces Application

Actor	Task	Sub-task	Notes
Administrator	1. Install WebCenter Portal and the back-end components for the Analytics and Activity Graph services		

Table 12–1 (Cont.) Configuring the Activity Graph Service for the Spaces Application

Actor	Task	Sub-task	Notes
	2. Configure a connection between WebCenter Portal: Spaces and the Analytics Collector using one of the following tools:		
		<ul style="list-style-type: none"> ■ Fusion Middleware Control ■ WLST 	
	3. (Optional) Set up the Activity Graph Engines schedule		
End User/ Administrator	4. Test that activity graph data is available in the Spaces application	<p>4.a Log in and interact with Spaces, for example, by adding content (End User)</p> <p>4.b Run the Activity Graph Engines (Administrator)</p> <p>4.c View recommendations in an Activity Graph task flow, for example, the Recommended Connections task flow on the Profile page (End User)</p>	

- **Roadmap - Configuring the Activity Graph Service for Framework applications**

The flow chart ([Figure 12–4](#)) and table ([Table 12–2](#)) in this section provide an overview of the prerequisites and tasks required to get the Activity Graph service working in Framework applications.

Figure 12-4 Configuring the Activity Graph Service for Framework Applications

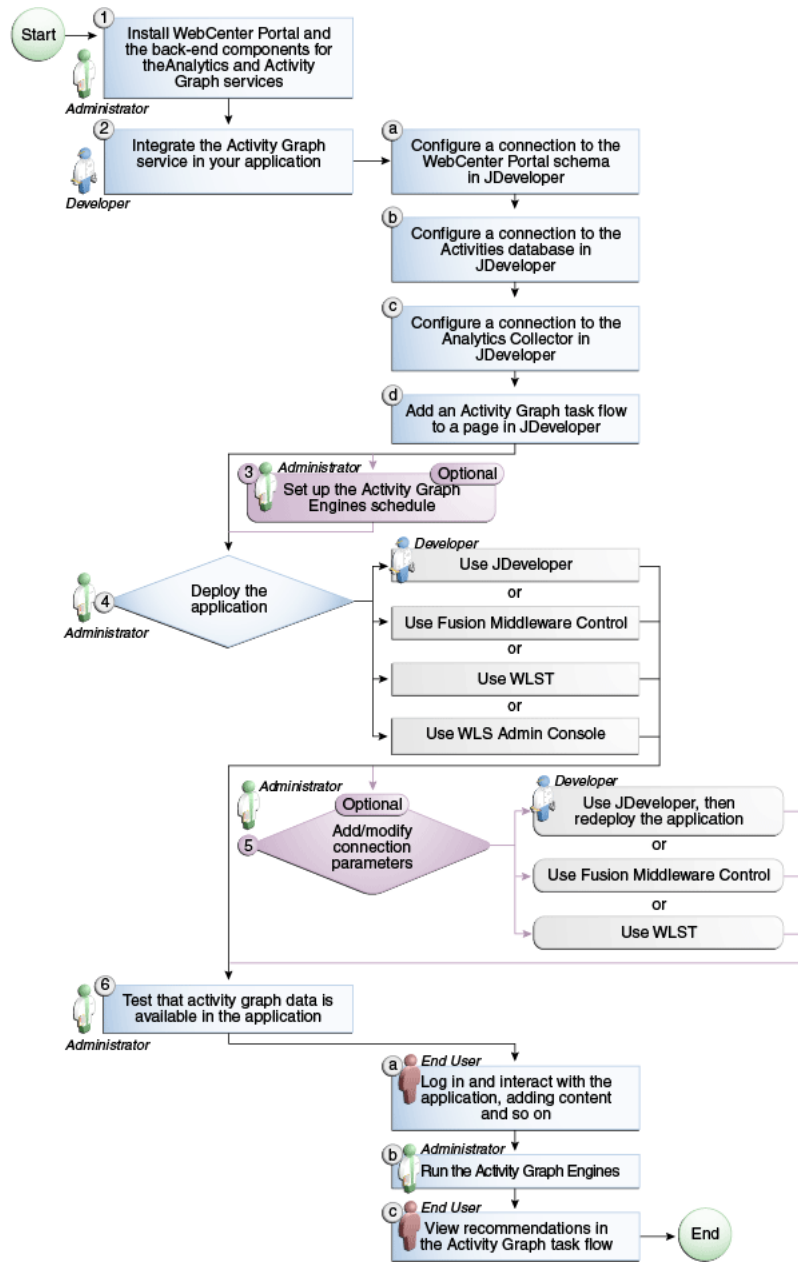


Table 12–2 Configuring the Activity Graph Service for Framework applications

Actor	Task	Sub-task	Notes
Administrator	1. Install WebCenter Portal and the back-end components for the Analytics and Activity Graph services		
Developer	2. Integrate the Activity Graph service in your application	2.a Configure a connection to the WebCenter Portal schema in JDeveloper 2.b Configure a connection to the Activities database in JDeveloper 2.c Configure a connection to the Analytics Collector in JDeveloper 2.d Add an Activity Graph task flow to a page in JDeveloper	
Administrator	3. (Optional) Set up the Activity Graph Engines schedule		
Developer/ Administrator	4. Deploy the application using one of the following tools: <ul style="list-style-type: none"> ■ JDeveloper (Developer) ■ Fusion Middleware Control (Administrator) ■ WLST (Administrator) ■ WLS Admin Console (Administrator) 		
Developer/ Administrator	5. (Optional) Add/modify connection parameters using one of the following tools: <ul style="list-style-type: none"> ■ JDeveloper, then redeploy the application (Developer) ■ Fusion Middleware Control (Administrator) ■ WLST (Administrator) 		
End User/ Administrator	6. Test that activity graph data is available in the application	6.a Log in and interact with the application, for example, by adding content (End User) 6.b Run the Activity Graph Engines (Administrator) 6.c View recommendations in the Activity Graph task flow, for example, the Recommended Connections task flow on your Profile page (End User)	

12.3 Activity Graph Service Prerequisites

The Activity Graph service requires that the Activity Graph engines application has been installed and configured. For more information, see the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Portal*.

In addition, in your application you must create a connection to the WebCenter Portal schema and to the Activities database. For more information, see the section "Setting

Up a Database Connection" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

The application must be configured to send usage events to the Analytics Event Collector. For more information, see [Section 13.5, "Registering an Analytics Collector for Your Application."](#)

Before the Activity Graph service can make recommendations, the Activity Graph engines must have been run at least once to gather the data and calculate similarity scores. For more information see [Section 12.4, "Preparing Data for the Activity Graph Service."](#)

The items suggested in the Similar Items task flow depend on the services that are available in your application. For example, documents are only recommended if the Documents service is available. For information about making a service available in your application, refer to the appropriate chapter for that service. An item can also be filtered out of the recommendations by the Resource Authorizer of the service that owns the item.

In a cluster environment, all instances of the Activity Graph engines application should be disabled except for one. For more information, see the section "Configuring Activity Graph" in the *Oracle Fusion Middleware High Availability Guide*.

12.4 Preparing Data for the Activity Graph Service

The Activity Graph engines consist of three separate engines for gathering data, calculating similarity scores, and calculating search rankings. These engines are:

- The Gathering Engine—gathers activities from the Analytics tables and other repositories via a set of registered activity providers.
- The Collaborative Filtering Engine (CFE)—calculates similarity scores on pairs of objects and stores them in the activity graph for later generation of similarity recommendations. It does this by performing a set of similarity calculations. Similarity calculations are objects that tell the Collaborative Filtering Engine how to calculate similarity scores on a given set of domain and background node classes. Each resulting similarity score is a number between 0 and 1 designating how similar two objects are to each other given a specific criterion. Similarity calculations are specified by the following properties: their domain and background classes, a distance function, and a relation combination.
- The Rank Engine—calculates a measure of importance of every node in the activity graph. These activity ranks can be stored in a search index and combined at query time with a query-dependent score to order search results. For more information, see [Section 12.7, "Setting Up Activity Rank for Oracle Secure Enterprise Search."](#) These scores are also useful in ordering context-free recommendations. For this reason, they are also stored in the Relation Store.

Before the Activity Graph service can begin to recommend objects, these engines must be run at least once to gather the data and calculate similarity scores. After this initial run, the engines can be run on demand, or on a schedule to ensure that new activities are captured and analyzed.

This section includes the following subsections:

- [Section 12.4.1, "Running the Activity Graph Engines on a Schedule"](#)
- [Section 12.4.2, "Running the Activity Graph Engines on Demand"](#)

12.4.1 Running the Activity Graph Engines on a Schedule

You can run the Activity Graph engines on a schedule to ensure that new activities are captured and analyzed on a regular basis. This is useful for applications with heavy traffic and frequently updated content.

To run the Activity Graph engines on a schedule:

1. Log in to Fusion Middleware Control and navigate to the home page for the WebCenter Portal application.
2. Using the navigation pane, navigate to **WebCenter>Portal>Activity Graph Engines>Activity Graph (WC_Uilities)>activitygraph-engines**.
3. Under **Web Modules**, click the URL for the Activity Graph Schedule and Status Page and log in.

Note: To access this page, you must be a member of the `Administrators` group.

The Activity Graph Schedule and Status page does not support multibyte user names and passwords, so you must log in using an ASCII-only user name and password.

Tip: You can access the Activity Graph Schedule and Status page directly by going to the following URL:

`http://host:port/activitygraph-engines`

where `http://host:port` is the URL for the `WC_Uilities` managed server.

4. On the Activity Graph Schedule and Status page, select **Run on a schedule**.
5. In the **Start on** field, enter the date on which you want the schedule to start.
6. In the **Run every** field, enter a value to determine how regularly the process occurs. For example, to run the process every day, enter 1 in the field. To run the process every other day, enter 2 in the field, and so on.
7. From the **at** dropdown list, select the time of day at which you want the process to start.
8. Click **Start**.

The process will run on the date specified at the time selected, and then will continue to run as you have scheduled.

12.4.2 Running the Activity Graph Engines on Demand

If the data in your application is not likely to change very frequently, you can run the Activity Graph engines on demand as and when required. You can also use this option to run the Activity Graph engines on demand in between regularly scheduled runs.

To run the Activity Graph engines on demand:

1. Log in to Fusion Middleware Control and navigate to the home page for the WebCenter Portal application.
2. Using the navigation pane, navigate to **WebCenter>Portal>Activity Graph Engines>Activity Graph (WC_Uilities)>activitygraph-engines**.

3. Under **Web Modules**, click the URL for the Activity Graph Schedule and Status Page and log in.

Note: To access this page, you must be a member of the Administrators group.

The Activity Graph Schedule and Status page does not support multibyte user names and passwords, so you must log in using an ASCII-only user name and password.

Tip: You can access the Activity Graph Schedule and Status page directly by going to the following URL:

`http://host:port/activitygraph-engines`

where `http://host:port` is the URL for the WC_Uutilities managed server.

4. Select **Run once now**.
5. Select **Incremental Update** to update the tables with any activities that occurred since the last time the Activity Graph engines ran.
Select **Full Rebuild** to delete all existing data and repopulate the tables with all activities. This may take some time.
6. Click **Start**.
You can monitor the progress of the process in the Status section of the dialog.
7. Click **Stop** at any time to stop the process, if required.
8. If you want to return to a regular schedule after the on demand process has run, be sure to select **Run on a schedule**, check that the details are correct, and then click **Start** to resume the schedule.

12.5 Customizing Reason Strings for Similarity Calculations

Similarity calculations can have associated reason strings to help users understand why a particular recommendation was made. When a person or object is recommended, if the highest scoring related similarity calculation has an associated reason string, that string is displayed in the task flow. You can edit the reason strings provided for similarity calculations, or create additional strings.

Each similarity calculation can define two strings for each reason to provide singular and plural phrasing.

Reason strings can be customized with the following tokens:

- `{RECOMMENDED_ITEM}`—The name of the current recommended item.
- `{NUMBER_OF_ITEMS}`—The number of objects in common. This corresponds to the numerator of the component score.
- `{TOTAL_ITEMS}`—The total number of items in common. This corresponds to the denominator of the component score. The meaning depends on the similarity function associated with the top similarity URN.
- `{SIMILARITY_CALCULATION}`—The name of the top similarity calculation.

For example, the `user-connect` similarity calculation defines the following two reason strings:

```
reason-user-connect=You share {NUMBER_OF_ITEMS} connections with {RECOMMENDED_ITEM}.
```

```
reason-user-connect=You share {NUMBER_OF_ITEMS} connection with {RECOMMENDED_ITEM}.
```

To customize reason strings for similarity calculations:

1. Open the `UIBundle.properties` file.
2. Locate the reason string that you want to customize and edit it as required.
3. To create a new reason string, use the following format:

```
reason-similarity-calculation=string
```

4. Save the `UIBundle.properties` file.

12.6 Managing Activity Graph Schema Customizations

WebCenter Portal provides out-of-the-box integration with the Activity Graph service that includes metadata definitions for mapping WebCenter Portal service event data from Analytics. This metadata is automatically loaded the first time the Activity Graph engines application starts.

You can extend Activity Graph metadata to change how actions are gathered from Analytics by manipulating XML files. To work with the metadata, you must first export the data to an XML file. After editing the XML files, you can then import the metadata back into the Activity Graph service.

This section includes the following subsections:

- [Section 12.6.1, "Exporting Activity Graph Metadata"](#)
- [Section 12.6.2, "Exporting Provider Configuration"](#)
- [Section 12.6.3, "Importing Activity Graph Metadata"](#)
- [Section 12.6.4, "Deleting Activity Graph Metadata"](#)
- [Section 12.6.5, "Renaming Actions and Node Classes"](#)

For information about the ways you can extend Activity Graph metadata, see the section "Extending the Activity Graph Service" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

12.6.1 Exporting Activity Graph Metadata

Use the WLST command `exportAGMetadata` to export Activity Graph metadata definitions to an XML file. For command syntax and examples, see the section "exportAGMetadata" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For example:

```
exportAGMetadata(appName='activitygraph-engines',
directoryPath='/scratch/monty', definitionFileName='activityGraphMetaData.xml',
includeProviderConfigurations=1)
```

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

12.6.2 Exporting Provider Configuration

Use the WLST command `exportAGProviderConfiguration` to export provider configuration metadata, for a given provider, to an Activity Graph metadata definition file. For command syntax and examples, see the section "exportAGProviderConfiguration" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For example:

```
exportAGProviderConfiguration(appName='activitygraph-engines',
directoryPath='/scratch/monty',
definitionFileName='activityGraph-analytics-mappings.xml',
urn='oracle.webcenter.activitygraph.analytics')
```

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

12.6.3 Importing Activity Graph Metadata

Use the WLST command `importAGMetadata` to import Activity Graph metadata definitions from an XML file. For command syntax and examples, see the section "importAGMetadata" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

12.6.4 Deleting Activity Graph Metadata

Use the WLST command `deleteAllAGMetadata` to delete all the Activity Graph metadata that is defined for a WebCenter Portal application. You should use this command in conjunction with the WLST command `importAGMetadata` to completely reinstall Activity Graph metadata. For command syntax and examples, see the section "deleteAllAGMetadata" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

Note: You should use this command only if you plan to import a new set of metadata.

You can delete metadata for individual Activity Graph objects using the WLST command indicated:

- Node class (`deleteAGNodeClass`)
- Action (`deleteAGAction`)
- Similarity calculation (`deleteAGSimilarityCalculation`)
- Rank calculation (`deleteAGRankCalculation`)
- Provider assignment (`deleteAGProviderAssignment`)
- QRPP (`deleteAGQRPPRegistration`)

Note: These delete methods delete metadata from the schema. As a result of this, any associated data in the Activities database is removed the next time the Activity Graph engines are run.

For more information, see the section "Activity Graph" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

12.6.5 Renaming Actions and Node Classes

Use the WLST command `renameAGNodeClass` to change the URN of a node class currently registered with Activity Graph. For command syntax and examples, see the section "renameAGNodeClass" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

Use the WLST command `renameAGAction` to change the URN of an action currently registered with Activity Graph. For command syntax and examples, see the section "renameAGAction" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

Note: These commands do not delete any metadata associated with the affected node class or action

12.7 Setting Up Activity Rank for Oracle Secure Enterprise Search

Enterprise content contributed through WebCenter Portal and Fusion applications has a rich structure that lends itself to using the Markov Chain Analysis mathematical technique. This technique is used by the Rank Engine to produce an *Activity Rank* for each node that improves end user searches by producing more relevant result sets. This is achieved by introducing a measure of the importance of various objects into the Oracle Secure Enterprise Search (Oracle SES) search index. This importance can then be factored into how results are ordered in combination with more standard search criteria (term frequency, and so on). The determination of an object's importance is predicated on the history of users' interactions with that object.

With Activity Rank, the importance of a person depends on the number of items the person creates and edits; the importance of those items; the number of people who connect with the person; and the importance of those people. The importance of an item depends on the importance of its author; the number of people who view, tag, and edit the item; and the importance of those people.

The Rank Engine process can be divided into four phases:

- Gathering—The Rank Engine queries the Analytics store for data about the connections between users and documents.
- Reshaping—The data is transformed into a matrix.
- Multiplying—The matrix is used to calculate Activity Ranks.
- Result storage—The Activity Ranks are stored in the Oracle SES search server so that they can be used at search time.

Candidates for Activity Rank are limited to an intersection of WebCenter Portal: Spaces objects having Oracle SES crawler implementations, WebCenter Portal Analytics instrumentation, and registration for Activity Graph rank calculation.

For an object to receive an Activity Rank that will affect search behavior, it must be eligible to have its event data collected from Analytics, a rank computation generated by Activity Graph, and an indexed entry in search with the value of the attribute `wc_serviceId` matching one of the classes registered in Activity Graph. The currently supported objects are:

- Users
- Documents
- Blog entries
- Wiki pages

Note: Ranks are still calculated and used even in the case where the class of object is not searchable itself.

The range of actions considered for computing Activity Rank are defined in the `rankCalculation` specified in the `activityGraphMetaData.xml` file. The out-of-the-box declaration includes the following user actions:

```
<component actionURN="connect" weight="10.0"/>
<component actionURN="edit" weight="20.0" inverse="true"/>
<component actionURN="view-count" weight="1.0"/>
<component actionURN="create" weight="100.0" inverse="true"/>
<component actionURN="create" weight="100.0"/>
<component actionURN="edit-count" weight="20.0"/>
<component actionURN="download" weight="5.0"/>
<component actionURN="tag" weight="10.0"/>
<component actionURN="comment" weight="10.0"/>
```

From this you can see that the single action of viewing a document conveys significantly less importance (`weight="1.0"`) to that document than the act of creating (`weight="100.0"`) or tagging (`weight="10.0"`) the document.

Additionally, when the `inverse` attribute is set to `true`, a relationship from object-to-user is denoted. The effect of this relationship is to enable users to accrue authority from objects whose rank appreciates. For example, the author of a document (a `create` relationship) collects rank from that document as its rank appreciates from actions performed by other users on that document—tagging, viewing, downloading—which then amplifies the weight of the user’s future actions.

When the Activity Graph Rank Engine completes its rank calculation for all of the affected objects, it sends a resulting set of identifiers with normalized ranks between 1 and 10 to a plug-in class, the `SesRankResultAcceptor`. This class simply pushes the ranks into the search index using the Oracle SES SOAP API. Once accepted by the SOAP API, the ranks, or *docscores* as they are known in Oracle SES, are immediately factored into the search ranking (providing the `DocScore` feature is fully enabled).

So, for two or more items within the same strata of a result set, those with higher docscores will receive higher search scores than they would otherwise, potentially raising them to a higher rank within that strata.

Before You Begin

Since Activity Rank works in conjunction with Oracle SES, you must make sure that Oracle SES is installed and configured correctly. Also, as Activity Rank only affects searchable items, the Rank Engine should be run after the SES crawler has finished a

run. For more information, see the chapter "Managing the Search Service" in *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal*.

To configure Activity Rank for Oracle SES:

1. The Rank Engine expects to use docscore attributes with external names of DOC_SCORE_1 for ACTIVITY-RANK and DOC_SCORE_2 for LIKE-RANK. Therefore, you must perform a one-time mapping call to establish these fields by calling the stored procedure `eq_sdata.create_sdata_attribute`:

```
exec eq_sdata.create_sdata_attribute('ACTIVITY-RANK');
exec eq_sdata.create_sdata_attribute('LIKE-RANK');
```

Note: These stored procedures must be invoked from the server hosting the Oracle SES instance.

2. You must also add entries for these attributes to the Oracle SES `ranking.xml` file to determine the weight that they carry.

For Oracle SES 11.1.2.2, add the following:

```
<ranking>
  <docscore-factor>
    <attribute-name>ACTIVITY-RANK</attribute-name>
    <column-name>DOC_SCORE_1</column-name>
    <weight>1.0</weight>
  </docscore-factor>
  <docscore-factor>
    <attribute-name>LIKE-RANK</attribute-name>
    <column-name>DOC_SCORE_2</column-name>
    <weight>1.0</weight>
  </docscore-factor>
</ranking>
```

For all other versions of Oracle SES, add the following:

```
<ranking>
  <docscore-factor>
    <attribute-name>ACTIVITY-RANK</attribute-name>
    <column-name>DOC_SCORE_1</column-name>
    <weight>1.0</weight>
  </docscore-factor>
  <docscore-factor>
    <attribute-name>LIKE-RANK</attribute-name>
    <column-name>DOC_SCORE_2</column-name>
    <weight>1.0</weight>
  </docscore-factor>
  <docscore-factor>
    <attribute-name>Doc_Score</attribute-name>
    <weight>1.0</weight>
  </docscore-factor>
</ranking>
```

Tip: The `ranking.xml` file is located in the following directory:

```
$SES_HOME/search/webapp/config
```

3. Restart the Oracle SES middle tier so that the changes take effect.
4. Use the WLST command `setAGProperty` to set the following Activity Graph properties:

```
oracle.webcenter.activitygraph.providers.datasources.ses.soap.admin.url
oracle.webcenter.activitygraph.providers.datasources.ses.soap.query.url
```

For example:

```
setAGProperty(appName='activitygraph-engines',
propertyName='oracle.webcenter.activitygraph.providers.datasources.ses.soap.adm
in.url',
propertyValue='http://seshostname:7777/search/api/admin/AdminService',
propertyType='String')
```

```
setAGProperty(appName='activitygraph-engines',
propertyName='oracle.webcenter.activitygraph.providers.datasources.ses.soap.que
ry.url',
propertyValue='http://seshostname:7777/search/query/OracleSearch',
propertyType='String')
```

Setting these properties enables the `SESRankResultAcceptor` to connect to the Oracle SES server and record ranks in the index.

5. Use the WLST command `setAGPasswordCredential` to set the user names and passwords to use to access the URLs defined by the two properties.

Note: The credentials should match a user that has access to all searchable items.

For example:

```
setAGPasswordCredential(appName='activitygraph-engines',
propertyName='oracle.webcenter.activitygraph.providers.datasources.ses.soap.adm
in.credential',
userName='eqsys',
password='welcome1')
```

```
setAGPasswordCredential(appName='activitygraph-engines',
propertyName='oracle.webcenter.activitygraph.providers.datasources.ses.soap.que
ry.credential',
userName='orcladmin',
password='welcome1')
```

6. Restart the managed server on which the Activity Graph engines application is deployed (that is, the `WC_Uutilities` managed server).

12.8 Troubleshooting Issues with Recommendations

This section provides information to assist you in troubleshooting problems you may encounter while using the Activity Graph service.

Note: The following troubleshooting solutions assume that the Activity Graph engines are deployed correctly, the `WC_Uutilities` managed server is up and running, and the property `openusage enabled` is `true`.

You should also ensure that you have read [Section 12.3, "Activity Graph Service Prerequisites."](#)

12.8.1 Troubleshooting the Activity Graph Engines Schedule and Status Page

Problem

The Activity Graph Schedule and Status page throws an error while running the Activity Graph engines

Solution

Basic verification in this case is to verify the deployment status of the Activity Graph engines from the WebLogic Console.

Problem

When the Activity Graph engines are started from the Schedule and Status page, the status of the engines is not reflected in the UI.

Solution

Check the Activity Graph logs to verify whether the engines are actually running or not. If the logs show that the engines are running, then the issue is only with the UI and it will not have any effect on the recommendations being displayed in the task flows. If the logs do not show any entries for the gathering/CFE engines, then there might be a problem with the event mapping file.

Tip: The Activity Graph engines logs can be found in:

domain/log/WC_Uutilities.out

domain/servers/WC_Uutilities/logs/WC_Uutilities-diagnostics.log

Problem

Cannot log in to the Activity Graph Schedule and Status page.

Solution

The Activity Graph Schedule and Status page does not support multibyte user names or passwords. Log in as an administrator with an ASCII-only user name and password.

Managing the Analytics Service

This chapter describes how to configure and manage the Analytics service for WebCenter Portal applications. The Analytics service enables you to display usage and performance metrics for these applications.

Always use Fusion Middleware Control or the WLST command-line tool to review and configure back-end services for WebCenter Portal applications. Any changes that you make to *WebCenter Portal applications*, post deployment, are stored in the MDS metadata store as customizations. See [Section 1.3.5, "WebCenter Portal Configuration Considerations."](#) Any changes that you make to *Analytics Collector* configuration are stored in the Analytics database.

Note: Changes that you make to Analytics service configuration, through Fusion Middleware Control or using WLST, are not dynamic so you must restart the managed server on which the Analytics Collector or the WebCenter Portal application is deployed for your changes to take effect. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

This chapter includes the following sections:

- [Section 13.1, "What You Should Know About Analytics in WebCenter Portal"](#)
- [Section 13.2, "Configuration Roadmap for the Analytics Service"](#)
- [Section 13.3, "Analytics Prerequisites"](#)
- [Section 13.4, "Configuring Analytics Collector Settings"](#)
- [Section 13.5, "Registering an Analytics Collector for Your Application"](#)
- [Section 13.6, "Configuring User Profile Events Timing"](#)
- [Section 13.7, "Validating Analytic Event Collection"](#)
- [Section 13.8, "Viewing the Current WebCenter Portal's Analytic Event List"](#)
- [Section 13.9, "Purging Analytics Data"](#)
- [Section 13.10, "Partitioning Analytics Data"](#)
- [Section 13.11, "Troubleshooting Issues with Analytics"](#)

Audience

The content of this chapter is intended for administrators who are responsible for setting up Analytics in WebCenter Portal, and configuring Analytics Collector details for Framework applications and Spaces.

13.1 What You Should Know About Analytics in WebCenter Portal

Analytics allows WebCenter Portal administrators and business users to track and analyze portal usage. Analytics provides the following basic functionality:

- **Usage Tracking Metrics:** Analytics collects and reports metrics for common portal functions, including community, page, portlet, and document visits.
- **Behavior Tracking:** Users can analyze portal metrics to determine usage patterns, such as portal visit duration and usage over time.
- **User Profile Correlation:** Users can correlate metric information with user profile information. Usage tracking reports can be viewed and filtered by user profile data such as country, company, or state. For more details, see "Query Options" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

An overview of Analytics components and ready-to-use task flows are described in the following sections:

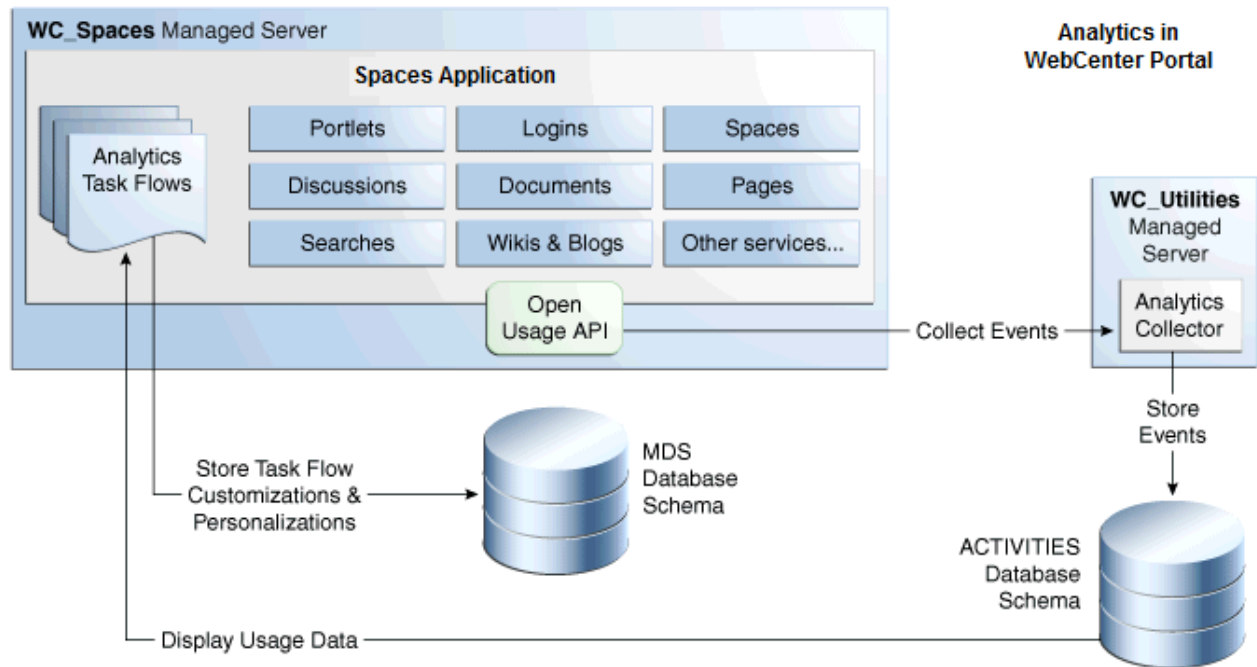
- [Section 13.1.1, "Analytics Components"](#)
- [Section 13.1.2, "Analytics Task Flows"](#)

13.1.1 Analytics Components

Figure 13–1 illustrates components for the Analytics service in WebCenter Portal:

- **WC_Spaces** - The managed server in which the Spaces application is deployed. (Framework applications are deployed on different managed servers.)
- **WC_Uilities** - The managed server in which the Analytics Collector is deployed.
- **Event Data** - Analytics tracks and collects a defined set of events. A comprehensive set of the most common events are provided out-of-the-box.
- **Open Usage API** - The OpenUsage API sends metrics to the Analytics Collector using UDP (User Datagram Protocol).
- **Analytics Collector** - The Analytics Collector component gathers event data. Analytics Collectors can be clustered to provide increased scalability and reliability.
- **Analytics Database** - The Analytics database (ACTIVITIES) stores metrics gathered from portal and non-portal events.
- **Analytics Task Flows** - Analytics provides a series of task flows to report metrics for common portal functions.
- **MDS** - The Oracle Metadata Service (MDS) repository that stores task flow customizations.

Figure 13–1 Analytics Components



13.1.2 Analytics Task Flows

Table 13–1 lists the Analytics task flows available with WebCenter Portal. The task flows work similarly for Framework applications and Spaces. For detailed information about these task flows and how to use them, see "Understanding Analytics Task Flows in Spaces" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

Table 13–1 Analytics Task Flows in WebCenter Portal

Analytics Task Flows	Description
WebCenter Portal Traffic	A summarized view for common events within the portal.
Page Traffic	Displays the number of page visits and the number of unique users that visited any page within the portal.
Login Metrics	Reports portal logins.
Portlet Traffic	Displays usage data for a portlet.
Portlet Response Time	Displays performance data for a portlet.
Portlet Instance Traffic	Displays usage data for a portlet instance. When the same portlet displays on several different pages, each placement is considered as a portlet instance.
Portlet Instance Response Time	Displays performance data for a portlet instance.
Search Metrics	Tracks portal searches.
Document Metrics	Tracks document views.
Wiki Metrics	Tracks most popular/least popular wikis.
Blog Metrics	Tracks most popular/least popular blogs.

Table 13–1 (Cont.) Analytics Task Flows in WebCenter Portal

Analytics Task Flows	Description
Discussion Metrics	Tracks most popular/least popular discussions.
Space Traffic*	(Spaces only) Displays usage data for a space.
Space Response Time*	(Spaces only) Displays page performance data for a space.

* These task flows are specific to Spaces. These task flows are not available for Framework applications.

13.2 Configuration Roadmap for the Analytics Service

The flow chart depicted in Figure 13–2 and Table 13–2 provides an overview of the prerequisites and tasks required to get the Analytics service working in the Spaces application.

Figure 13–2 Configuring the Analytics Service for Use in the Spaces Application

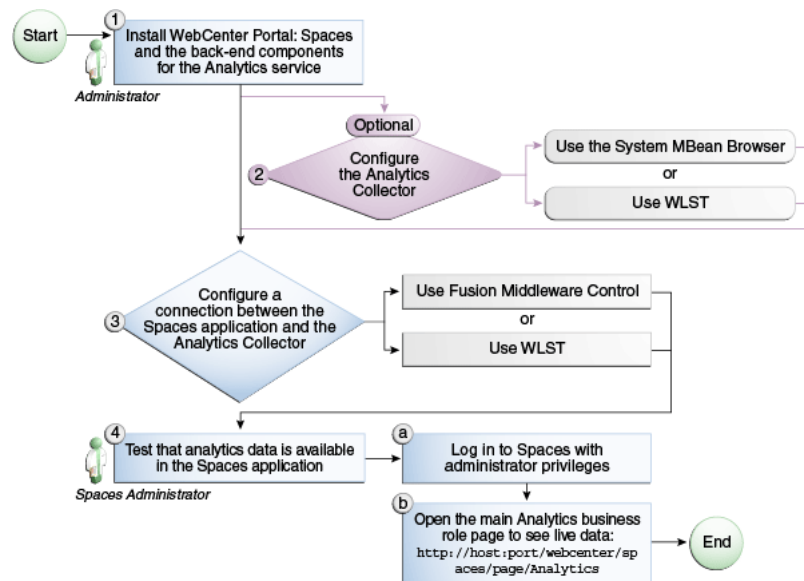


Table 13–2 Configuring the Analytics Service for Use in Spaces

Actor	Task	Sub-task
Administrator	1. Install Oracle WebCenter Portal: Spaces and the back-end components for the Analytics service	
Administrator	2. (Optional) Configure the Analytics Collector using either of the following tools:	<ul style="list-style-type: none"> ■ System MBean Browser ■ WLST

Table 13–2 (Cont.) Configuring the Analytics Service for Use in Spaces

Actor	Task	Sub-task
Administrator	3. Configure a connection between the Spaces application and the Analytics Collector using either of the following tools: <ul style="list-style-type: none"> ■ Fusion Middleware Control ■ WLST 	
Spaces Administrator	4. Test that analytics data is available in Spaces	4.a Log in to Spaces with administrator privileges 4.b Open the main Analytics business role page to see live data: http://host:port/webcenter/spaces/page/Analytics

13.3 Analytics Prerequisites

This section includes the following subsections:

- [Section 13.3.1, "Analytics - Installation"](#)
- [Section 13.3.2, "Analytics - Configuration"](#)
- [Section 13.3.3, "Analytics - Security Considerations"](#)
- [Section 13.3.4, "Analytics - Limitations"](#)

13.3.1 Analytics - Installation

The Analytics Collector is an optional installation option for Oracle WebCenter Portal. To install this product, select **Oracle WebCenter Portal Analytics Collector** in the Fusion Middleware Configuration Wizard. For detailed installation instructions, see *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Portal*.

The Analytics schema (ACTIVITIES) and the WebCenter Portal schema (WEBCENTER) can be installed on the same database or on separate databases.

13.3.2 Analytics - Configuration

The Analytics Collector is configured to receive events out-of-the-box, using installation defaults. If the default values are not suitable for your installation or you have a cluster, you may configure different values using WLST or MBeans Browser. For more details, [Section 13.4, "Configuring Analytics Collector Settings."](#)

Out-of-the-box, Spaces is not configured to *send events* to the Analytics Collector. If you want to collect usage and performance metrics for Spaces (or any Framework application) you must register the Analytics Collector and enable event collection. For more details, see [Section 13.5, "Registering an Analytics Collector for Your Application."](#) Once connected, analytics data is collected and displays in your application (through Analytics task flows) without further configuration.

13.3.3 Analytics - Security Considerations

In Spaces, Resource Catalogs only display Analytics task flows to users with appropriate permissions:

- Administrators - Users with the Administrator role have access to all Analytics task flows
- Moderators - Within a particular space, members with the Moderator role have access to Analytics task flows that display usage data for that space only

Analytics usage data is valuable for portal analysis but might be regarded as private or sensitive to portal users. To protect security and privacy interests associated with usage metrics Spaces administrators and individual space moderators must manage page security such that only appropriate, specified users have access to pages that expose analytics data. See also, "Securing Pages and Components" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

Similarly, developers building Framework applications must set up a suitable security model for exposing Analytics task flows and data. For details, see "Setting up Security for Analytics Task Flows and Usage Data" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

13.3.4 Analytics - Limitations

Analytics task flows do not display custom event information.

13.4 Configuring Analytics Collector Settings

During installation, the Analytics Collector is configured to receive events using the following default values:

- **Collector Host Name** - localhost
- **Default Port** - 31314
- **Maximum Port Number** - 31314
- **Broadcast Type** - Multicast
- **Clustering** - The clustering settings do not apply. Clustering is not supported in this version.

If these default values are not suitable for your installation or you have a cluster, you can configure suitable values using WLST or the MBeans Browser in Fusion Middleware Control:

- [Setting Analytics Collector Properties Using WLST](#)
- [Setting Analytics Collector Properties Using Fusion Middleware Control](#)

These Analytics Collector configuration settings are stored in the Analytics database (ACTIVITIES).

13.4.1 Setting Analytics Collector Properties Using WLST

Use the WLST command `setAnalyticsCollectorConfig` to set event collection properties for the Analytics Collector. For command syntax and examples, see the section, "setAnalyticsCollectorConfig" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

Note: To start using the property values you must restart the managed server on which the Analytics Collector application is deployed (WC_Uilities). For more information, see the section, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

13.4.2 Setting Analytics Collector Properties Using Fusion Middleware Control

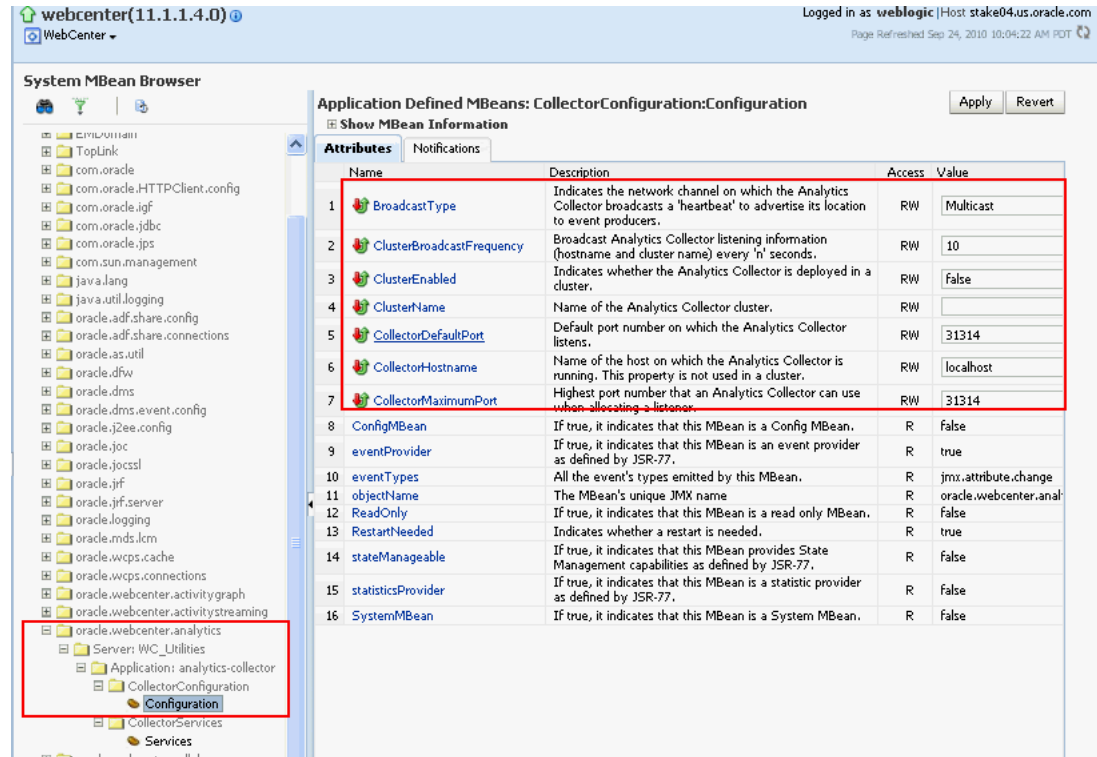
Use the Systems MBeans Browser in Fusion Middleware Control to set event collection properties for the Analytics Collector:

To configure the Analytics Collector (deployed on the WC_Uilities managed server):

1. Log in to Fusion Middleware Control and navigate to the home page for Spaces or your Framework application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Open the System MBean Browser:
 - For the Spaces application- From the **WebCenter Portal** menu, choose **System MBean Browser**.
 - For Framework applications - From the **Application Deployment** menu, choose **System MBean Browser**.
3. Navigate to:
Application Defined MBeans >oracle.webcenter.analytics >Server: WC_Uilities >Application: analytics-collector >CollectorConfiguration >Configuration

Alternatively, search for CollectorConfiguration or filter the System MBean Browser tree using the MBean pattern: `oracle.webcenter.analytics:*`

Figure 13–3 System MBeans Browser - Analytics Collector Properties



4. Modify configuration properties for the Analytics Collector. For details, see [Table 13–3](#).

Table 13–3 Analytics Collector - Configuration Properties

Field	Description
BroadcastType	Specify the network channel on which the Analytics Collector broadcasts a 'heartbeat' to advertise its location to event producers. Valid values are Broadcast and Multicast : Broadcast - use the standard network broadcast channel. Multicast - use a special fixed multicast address.
CollectorHostName	Enter the name of the host on which the Analytics Collector is running. The default setting is localhost.
CollectorDefaultPort	Enter the default port number on which the Analytics Collector listens. The default value is 31314.
CollectorMaximumPort	Enter the highest port number that an Analytics Collector can use when allocating a listener. This property is mostly used in a clustered environment where multiple collectors run in the same box. Each collector listens for incoming UDP messages on a free port within a given port range. The range is from the default port number to the maxPort number.
ClusterEnabled	The clustering settings do not apply. Clustering is not supported in this version.
ClusterName	The clustering settings do not apply. Clustering is not supported in this version.

Table 13–3 (Cont.) Analytics Collector - Configuration Properties

Field	Description
HeartbeatFrequency	The clustering settings do not apply. Clustering is not supported in this version.

- To start using the new settings you must restart the managed server on which the Analytics Collector application is deployed (`WC_Utilities`). For more information, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

13.5 Registering an Analytics Collector for Your Application

Events raised in Spaces or a Framework application using OpenUsage APIs can be sent to an Analytics Collector for use by the Analytics service, Recommendations service, and the Activity Graph Engine. If you intend to use any of the features or task flows provided by these services you must connect Spaces or the Framework application to an Analytics Collector.

While you can register multiple Analytics Collector connections for Spaces or your Framework application, only one Analytics Collector is used - the default (or active) connection.

To start using a new configuration you must restart the managed server on which Spaces or your Framework application is deployed.

This section includes the following subsections:

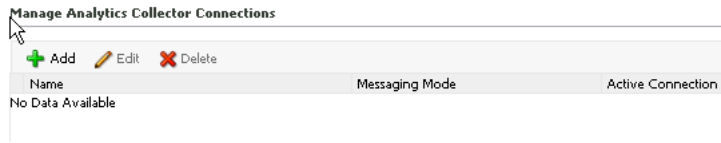
- [Section 13.5.1, "Registering an Analytics Collector Using Fusion Middleware Control"](#)
- [Section 13.5.2, "Registering an Analytics Collector Using WLST"](#)
- [Section 13.5.3, "Disabling WebCenter Event Collection"](#)

13.5.1 Registering an Analytics Collector Using Fusion Middleware Control

To register an Analytics Collector for Spaces or a Framework application:

- Log in to Fusion Middleware Control and navigate to the home page for Spaces or your Framework application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
- Open the Service Configuration page:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
- From the list of services on the WebCenter Portal Service Configuration page, select **Analytics and Activity Graph**.
- To connect to an Analytics Collector, click **Add** ([Figure 13–4](#)).

Figure 13–4 Configuring Analytics Collector Connections



5. Enter a unique name for this connection.
The name must be unique (across all connection types) within Spaces or your Framework application.
6. Select **Active Connection** to use this connection for Analytics and Activity Graph services.
While you can register multiple Analytics Collector connections for Spaces or your Framework application, only one connection is used—the default (or active) connection.
7. Select **Enable WebCenter Portal Event Collection** to send analytics events raised using OpenUsage APIs to the Analytics Collector.
Deselect this option if you do not want to collect analytics data.
8. Enter connection details for the Analytics Collector. For details, see [Table 13–4](#).

Table 13–4 Analytics Collector Connection - Connection Details

Field	Description
Messaging Mode	This property specifies whether to send events to a clustered Analytics Collector in multicast mode or a single Analytics Collector using unicast communication. Clustering the Analytics Collector is not supported in the current release, so the only valid value for this release is <code>Unicast</code> .
Collector Host Name	If the messaging mode is set to <code>Unicast</code> , enter the host name where the Analytics Collector is running. The default setting is <code>localhost</code> .
Collector Port	Enter the port on which the Analytics Collector listens for events. The default value is <code>31314</code> .
Cluster Name	If the messaging mode is set to <code>Multicast</code> , enter the name of the cluster where a clustered Analytics Collector is running.
Timeout (Seconds)	If the messaging mode is set to <code>Multicast</code> , enter the length of time (in seconds) to wait for a response from the Analytics Collector. The default value is 30 seconds.

9. Click **OK** to save.
10. To start using the new (active) connection you must restart the managed server on which Spaces or your Framework application is deployed. For more information, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

13.5.2 Registering an Analytics Collector Using WLST

Use the WLST command `createAnalyticsCollectorConnection` to create an Analytics Collector connection for Spaces or your Framework application. To update an existing connection, use `setAnalyticsCollectorConnection`. For command

syntax and examples, see the section, "createAnalyticsCollectorConnection" and "setAnalyticsCollectorConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

Note: To start using the new connection, ensure that `isEnabled=1` and `default=1`, and then restart the managed server on which Spaces or your Framework application is deployed. See, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

13.5.3 Disabling WebCenter Event Collection

If you do not want to collect events raised using OpenUsage APIs, you can stop event transmission temporarily or permanently.

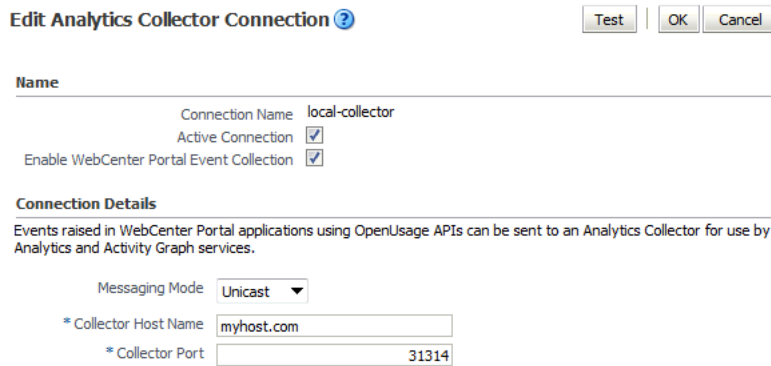
This section includes the following subsections:

- [Section 13.5.3.1, "Disabling WebCenter Portal Event Collection Using Fusion Middleware Control"](#)
- [Section 13.5.3.2, "Disabling WebCenter Portal Event Collection Using WLST"](#)

13.5.3.1 Disabling WebCenter Portal Event Collection Using Fusion Middleware Control

To disable event collection for Spaces or your Framework application:

1. Log in to Fusion Middleware Control and navigate to the home page for Spaces or your Framework application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Open the Service Configuration page:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
3. From the list of services on the WebCenter Portal Service Configuration page, select **Analytics and Activity Graph**.
4. Select the connection in the table, and then click **Edit**.
5. Deselect **Enable WebCenter Portal Event Collection** ([Figure 13-5](#)).

Figure 13–5 Disabling Analytics Event Collection


Edit Analytics Collector Connection Test OK Cancel

Name

Connection Name local-collector

Active Connection

Enable WebCenter Portal Event Collection

Connection Details

Events raised in WebCenter Portal applications using OpenUsage APIs can be sent to an Analytics Collector for use by Analytics and Activity Graph services.

Messaging Mode Unicast

* Collector Host Name myhost.com

* Collector Port 31314

- To effect this change you must restart the managed server on which Spaces or your Framework application is deployed. For more information, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

13.5.3.2 Disabling WebCenter Portal Event Collection Using WLST

To disable event collection using WLST, run the `setAnalyticsCollectorConnection` command with the `isEnabled` argument set to 0 (`false`). For command syntax and examples, see the section, "setAnalyticsCollectorConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

13.6 Configuring User Profile Events Timing

User profile information is cached, meaning that changes to a user profile are not visible in reports until the cache is updated. The cache is limited to 1000 objects by default, with each object remaining in the cache for 60 minutes by default. You can change these values using WLST. To change the maximum number of objects in the cache, run the `setProfileCacheNumberOfObjects` command. To change the time an object remains idle in the cache, run the `setProfileCacheTimeToLive` command.

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

13.7 Validating Analytic Event Collection

You can check whether events reach the Analytics Collector by checking the trace log at:

```
<base_domain_name>/servers/WC_Uutilities/logs/analytics-collector/collector.trc
```

Event messages are similar to the following:

```
[2010-09-16T07:13:56.906-07:00] [WC_Uutilities] [TRACE] []
[SRC_METHOD: OnMessageReceived] Event = [[
EVENT_TYPE: {http://www.myorg.com/videoapp}VIDEOVIEWS
VERSION: 3.0.XXXX
AS_DIMENSION_USER.USERID: testuser01
```

```
VIDEO.RESOURCEID: video8736
VIDEO.TITLE: Project Kick Off
VIDEO.LOOP: false
QUALITY: 720
PROPERTY_VERSION: 3.0.XXXX
```

To display analytics collector configuration information, enter the following URL:

```
http://hostname:WC_Uilities_port/collector
```

This page lists the following:

- Collector Default Port
- Collector Max Port
- Collector Server Name
- Broadcast Type
- Cluster Enabled
- Cluster Name
- Partitioning Enabled
- Time Dimension for This Year
- Space Dimension Exists (for Spaces application installations)

13.8 Viewing the Current WebCenter Portal's Analytic Event List

Use the Systems MBeans Browser in Fusion Middleware Control to see which events that an Analytics Collector is configured to collect.

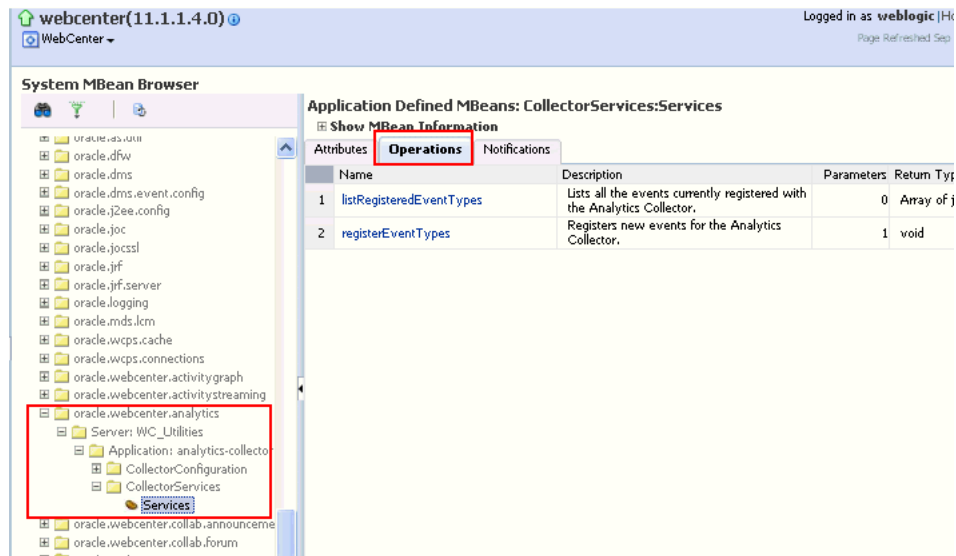
To display the current list of analytics events:

1. Log in to Fusion Middleware Control and navigate to the home page for Spaces or your Framework application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Open the System MBean Browser:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **System MBean Browser**.
 - For Framework applications - From the **Application Deployment** menu, choose **System MBean Browser**.
3. Navigate to:


```
Application Defined MBeans> oracle.webcenter.analytics Server: WC_Uilities>
Application: analytics-collector> CollectorServices> Services
```

Alternatively, search for `CollectorServices` or filter the System MBean Browser tree using the MBean pattern: `oracle.webcenter.analytics:*`

4. Select the **Operations** tab.

Figure 13–6 System MBeans Browser - Register Analytics Events

5. Click `listRegisteredEventTypes`.
6. Click `Invoke`.

Alternatively, use the WLST command `listAnalyticsEventTypes`. For command syntax and examples, see the section, "listAnalyticsEventTypes" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

13.9 Purging Analytics Data

For more information, see "Purging Oracle WebCenter Portal Analytics Data" in the *Oracle Fusion Middleware Administrator's Guide*.

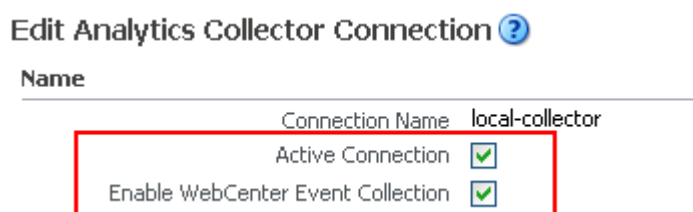
13.10 Partitioning Analytics Data

For more information, see "Partitioning Oracle WebCenter Portal Analytics Data" in the *Oracle Fusion Middleware Administrator's Guide*.

13.11 Troubleshooting Issues with Analytics

If users cannot see analytics in Spaces or your Framework application, verify the following:

- Check that the Analytics Collector configuration is correct and in particular that both **Enable WebCenter Event Collection** and **Active Connection** are both set (Figure 13–7). See [Registering an Analytics Collector for Your Application](#).

Figure 13–7 Enabling the Connection and Analytics Collection

If you make changes to the connection you must restart the managed server on which Spaces or your Framework application is deployed. For more information, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

- If Spaces or your Framework application was recently upgraded, verify that the domain startup script does not contain legacy Analytics Collector settings as these values override any connection details that you specify through Fusion Middleware Control or using WLST.
 1. Shut down the managed server on which Spaces or your Framework application is deployed.
 2. Edit the domain startup script `setDomainEnv` located at:
 - UNIX: `DOMAIN_HOME/bin/setDomainEnv.sh`
 - Windows: `DOMAIN_HOME\bin\setDomainEnv.cmd`
 3. Remove Analytics Collector settings.
 4. Restart the managed server.

Managing the Announcements and Discussions Services

This chapter describes how to configure and manage the Announcements and Discussions services for your application. These two services use the same connection to Oracle WebCenter Portal's Discussion Server.

Unless otherwise documented, do not make configuration changes within Oracle WebCenter Portal's Discussion Server. Always use Fusion Middleware Control or the WLST command-line tool to review and configure back-end services for WebCenter Portal applications. For troubleshooting tips with Oracle WebCenter Portal's Discussion Server, see [Section 14.12, "Troubleshooting Issues with Announcements and Discussions."](#)

Any changes that you make to applications, post deployment, are stored in MDS metadata store as customizations. See [Section 1.3.5, "WebCenter Portal Configuration Considerations."](#)

Note: Configuration changes for the Discussions and Announcements services, through Fusion Middleware Control or using WLST, are not dynamic so you must restart the managed server on which your application is deployed for changes to take effect. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

This chapter includes the following sections:

- [Section 14.1, "What You Should Know About Discussions Server Connections"](#)
- [Section 14.2, "Discussions Server Prerequisites"](#)
- [Section 14.3, "Registering Discussions Servers"](#)
- [Section 14.4, "Choosing the Active Connection for Discussions and Announcements"](#)
- [Section 14.5, "Modifying Discussions Server Connection Details"](#)
- [Section 14.6, "Deleting Discussions Server Connections"](#)
- [Section 14.7, "Setting Up Discussions Service Defaults"](#)
- [Section 14.8, "Setting Up Announcements Service Defaults"](#)
- [Section 14.9, "Testing Discussions Server Connections"](#)
- [Section 14.10, "Granting Administrator Permissions on the Discussions Server"](#)

- [Section 14.11, "Granting Administrator Role on the Discussions Server"](#)
- [Section 14.12, "Troubleshooting Issues with Announcements and Discussions"](#)

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."](#)

14.1 What You Should Know About Discussions Server Connections

The Discussions service enables users to start, publish, and store discussions in your application. The Announcements service lets you create and expose announcements on your application pages.

The Discussions service and the Announcements service require a single connection to Oracle WebCenter Portal's Discussion Server. Both services use the same connection. Oracle WebCenter Portal's Discussion Server can be installed with Oracle Fusion Middleware.

You can register additional discussion server connections through the Fusion Middleware Control Console or using WLST, but only one connection is active at a time:

- [Section 14.3.1, "Registering Discussions Servers Using Fusion Middleware Control"](#)
- [Section 14.3.2, "Registering Discussions Servers Using WLST"](#)

WebCenter Portal: Spaces

Some additional configuration is required to use Discussions and Announcements services in the Spaces application. This includes choosing the category (on the discussions server) under which all Spaces discussions and announcements are stored, and more. This configuration takes place inside Spaces. For more information, see "Configuring Discussion Forum Options for Spaces" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

14.2 Discussions Server Prerequisites

This section includes the following subsections:

- [Section 14.2.1, "Discussions Server - Installation"](#)
- [Section 14.2.2, "Discussions Server - Configuration"](#)
- [Section 14.2.3, "Discussions Server - Security Considerations"](#)
- [Section 14.2.4, "Discussions Server - Limitations"](#)

14.2.1 Discussions Server - Installation

While installing Oracle WebCenter Portal, select to install Oracle WebCenter Portal's Discussion Server. Use the Repository Creation Utility (RCU) to create the DISCUSSIONS schema.

The Oracle Fusion Middleware Configuration Wizard automatically creates managed servers in the domain to host the selected WebCenter Portal components.

See Also: *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Portal*

14.2.1.1 Discussions Server - High Availability Installation

To set up Oracle WebCenter Portal's Discussion Server for high availability:

1. Install the WC_Collaboration domain in a clustered environment.
2. Log on to the discussions server admin console as an administrator by using the following URL format: `http://host:port/owc_discussions/admin`.
3. Go to the Cache Features page, and select to enable clustering (Figure 14–1).

Figure 14–1 Cache Features - Clustering

Feature	Status	Description
Short-term Query Cache	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled: object lifetime: <input checked="" type="radio"/> 5 seconds <input type="radio"/> 10 seconds	Prevents cache expirations of the query cache from happening more than once every 5 or 10 seconds. This is useful for sites with extreme amounts of traffic. The ramification to using the short-term query cache is that new content won't appear for 5 to 10 seconds after its posted.
Clustering	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	You can enable or disable clustered caching in the system. Note: enabling clustering may take up to 30 seconds.

Save Settings Cancel

14.2.2 Discussions Server - Configuration

There are numerous WLST commands for configuring the discussions server.

You can view, set, and remove Oracle WebCenter Portal's Discussion Server system properties with the following WLST commands:

- `getDiscussionsServerProperty`
- `setDiscussionsServerProperty`
- `removeDiscussionsServerProperty`

The `addDiscussionsServerAdmin` command grants system administrator permissions on the discussions server to a user or a group. This command is useful when you connect the discussions server to a new identity store that does not contain any of the current administrators. For command syntax and examples, see the section, "Discussions and Announcements" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

When you update Discussions or Announcements permissions for a space hierarchy, subspaces do not automatically inherit the corresponding permission changes on the discussions server. For subspaces to inherit discussions server permission changes applied to a parent, you must run the `syncDiscussionServerPermissions` command (WebCenter Portal: Spaces only). For command syntax and examples, see the section, "syncDiscussionsServerPermissions" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

Note: To execute discussions server WLST commands, such as `syncDiscussionServerPermissions`, the user used to connect to the admin server must also have administrative privileges on the discussions server.

14.2.3 Discussions Server - Security Considerations

- WS-Security establishes a trust relationship between your application and Oracle WebCenter Portal's Discussion Server so that your application can pass the user identity information to the discussions server without knowing the user's credentials.

Configure OWSM WS-Security for Oracle WebCenter Portal's Discussion Server, depending on your topology, following either [Section 34.1.3, "Configuring the Discussions Server for a Simple Topology,"](#) [Section 34.2.3, "Configuring the Discussions Server for a Typical Topology,"](#) or [Section 34.3.3, "Configuring the Discussions Server for a Complex Topology."](#)

- Oracle WebCenter Portal's Discussion Server-specific Web Services messages sent by WebCenter Portal applications to the discussions server are not encrypted. For message confidentiality, access the discussions server URL over Secure Socket Layer (SSL) or protect the Web Service end points with an OWSM policy. For more information, see [Chapter 33, "Configuring SSL"](#) and [Chapter 34, "Configuring WS-Security."](#)
- By default, Oracle WebCenter Portal's Discussion Server is configured to use the embedded LDAP identity store: All users in the embedded LDAP store can log on to the discussions server, and all users in the `Administrators` group have administrative privileges on the discussions server.

For your production environment, you must reassociate the identity store with an external LDAP server, as described in [Section 29.1, "Reassociating the Identity Store with an External LDAP Server."](#) In addition, you must either move the Fusion Middleware administrator account to the external LDAP (as described in [Section 29.5, "Moving the Administrator Account to an External LDAP Server"](#)), or if you choose not to move the administrator account, you must perform some additional steps to identify the new administrator account for the discussions server as described in [Section 29.5.1, "Migrating WebCenter Portal's Discussions Server to Use an External LDAP."](#)

- You can configure Oracle WebCenter Portal's Discussion Server to leverage single sign-on security using Oracle Access Manager, Oracle Single Sign-On, or SAML-based single sign-on. For information, see [Chapter 31, "Configuring Single Sign-on."](#) For additional Discussions-specific configuration instructions for Oracle Access Manager (OAM), see also [Chapter 31.2.6.2, "Configuring the Discussions Server for SSO."](#)

Note: If you set up SAML single sign-on, with WebCenter Portal: Spaces as the source application and Oracle WebCenter Portal's Discussion Server as the destination application, then you can access Oracle WebCenter Portal's Discussion Server administration pages from Spaces as follows:

- Space > Settings > Services page
- Administration > Configuration > Services page

However, because the administration pages of Oracle WebCenter Portal's Discussion Server do not participate in single sign-on, if you access the administration pages directly, you are required to log in to discussions server again.

- If WebCenter Portal is not integrated with a single sign-on solution, then different login sessions are required for the `owc_discussion` user (`/owc_discussions`) and the `owc_discussion` admin user (`/owc_discussions/admin`).
- User Identity: User identity management is handled by authentication providers settings specified in Oracle WebLogic Server using custom JPS Auth Factory. To check that the correct auth factory is running, go to Oracle WebCenter Portal's Discussions Server admin console Systems Properties page and confirm the following property values:
 - `owc_discussions.setup.complete_11.1.1.2.0=true`
 - `AuthFactory.className=oracle.jive.security.JpsAuthFactory`

If the `AuthFactory.className` is set to this value, then set the `owc_discussions.setup.complete_11.1.1.2.0` property to `false` and restart Oracle WebCenter Portal's Discussion Server. This ensures that proper initialization is done for the application.

14.2.4 Discussions Server - Limitations

Oracle WebCenter Portal's Discussion Server URL supports only English and Spanish languages for displaying labels; however, data can be entered in UTF-8 format. Oracle recommends using the WebCenter Portal application (with all supported languages) for user operations in the discussions server. All WebCenter Portal-supported languages are supported for data, such as discussion topics or announcements, and they are displayed in the discussions server also.

The Discussions and Announcements services do not support non-ASCII user names if the WebCenter Portal instance is running in a native encoding on Microsoft Windows. In a Linux environment, to allow support for non-ASCII user names in the Discussions and Announcements services, the server on which WebCenter Portal is deployed must have the environment variable `LC_ALL` set to `utf-8`.

WebCenter Portal: Spaces

Do not change user permissions in the discussions server, as this might cause unexpected behavior. Always manage user permissions for discussions and announcements in Spaces. For more information, see "Understanding Discussions Server Role Mapping" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

14.3 Registering Discussions Servers

You can register multiple discussions server connections for a WebCenter Portal application, but only one is active at a time.

To start using the new (active) connection you must restart the managed server on which the application is deployed.

This section includes the following subsections:

- [Section 14.3.1, "Registering Discussions Servers Using Fusion Middleware Control"](#)
- [Section 14.3.2, "Registering Discussions Servers Using WLST"](#)

14.3.1 Registering Discussions Servers Using Fusion Middleware Control

To register a discussions server:

1. Log in to Fusion Middleware Control and navigate to the home page for the application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
3. From the list of services on the WebCenter Portal Service Configuration page, select **Discussions and Announcements**.
4. To connect to a new discussions server, click **Add** ([Figure 14-2](#)).

Figure 14-2 Configuring Discussion and Announcement Connections



5. Enter a unique name for this connection, and indicate whether this connection is the active (or default) connection for the application ([Table 14-1](#)).

Table 14-1 Discussion and Announcement Connection - Name

Field	Description
Connection Name	Enter a unique name for the connection. The name must be unique (across all connection types) within the application.
Active Connection	Select to use this connection for the Discussions and Announcements services in the application. While you can register multiple discussions server connections for an application, only one connection is used for discussion and announcement services—the default (or active) connection.

6. Enter connection details for the discussions server. For details, see [Table 14-2](#).

Table 14-2 Discussion and Announcement Connection - Connection Details

Field	Description
Server URL	Enter the URL of the discussions server hosting discussion forums and announcements. For example: <code>http://discuss-server.com:8890/owc_discussions</code>

Table 14–2 (Cont.) Discussion and Announcement Connection - Connection Details

Field	Description
Administrator User Name	<p>Enter the user name of the discussions server administrator.</p> <p>This account is used by the Discussions and Announcements services to perform administrative operations on behalf of WebCenter Portal users.</p> <p>In the Spaces application, this account is mostly used for managing space-related discussions and announcements. It is not necessary for this user to be a super admin. However, the user must have administrative privileges on the current root category for WebCenter Portal: Spaces, that is, the category (on the discussions server) under which all space-related discussions and announcements are stored.</p> <p>Note: If your application does not include space-related functionality, then the administrator's user name is not required.</p>
Authenticated User Web Service Policy URI	<p>Select the policy this connection uses for authenticated access to the discussions server Web service.</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 has trust relationship with the receiver) vouches for the verification of the subject by method called sender-vouches.</p> <p>The client policy specified must be compatible with the service policy that is configured for the <code>OWCDiscussionsServiceAuthenticated</code> endpoint in the discussions server. Out-of-the-box, the default <i>service policy</i> is <code>WSS 1.0 SAML Token Service Policy (oracle/wss10_saml_token_service_policy)</code>.</p> <p>Options available are:</p> <ul style="list-style-type: none"> ■ WSS 1.0 SAML Token Client Policy (<code>oracle/wss10_saml_token_client_policy</code>) ■ WSS 1.1 SAML Token With Message Protection Client Policy (<code>oracle/wss11_saml_token_with_message_protection_client_policy</code>) ■ Global Policy Attachment <p>If your environment supports Global Policy Attachments, you must ensure that the default policy attached to the <code>OWCDiscussionsServiceAuthenticated</code> endpoint in the discussions server is set to <code>oracle/no_authentication_client_policy</code> using the WLST command <code>detachWebServicePolicy</code> or Enterprise Manager.</p>

Table 14–2 (Cont.) Discussion and Announcement Connection - Connection Details

Field	Description
Public User Web Service Policy URI	<p>Select the client policy this connection uses to enforce message security and integrity for public access to the discussions server Web service.</p> <p>The client policy specified must be compatible with the service policy that is configured for the <code>OWCDiscussionsServicePublic</code> endpoint in the discussions server. Out-of-the-box, a service policy is not configured for public access (None).</p> <p>Options available are:</p> <ul style="list-style-type: none"> ■ None - This is the default setting. ■ WSS 1.1 Message Protection Client Policy (<code>oracle/wss11_with_message_protection_client_policy</code>) ■ Global Policy Attachment <p>If your environment supports Global Policy Attachments, you must ensure that the default policy attached to the <code>OWCDiscussionsServicePublic</code> endpoint in the discussions server is set to <code>oracle/no_authentication_client_policy</code> using the WLST command <code>detachWebServicePolicy</code> or Enterprise Manager.</p>
Recipient Key Alias	<p>Enter the recipient key alias to be used for message protected policies (applicable to the <code>OWCDiscussionsServicePublic</code> and <code>OWCDiscussionsServiceAuthenticated</code> endpoints). This is the alias to the certificate that contains the public key of the discussions server in the configured keystore.</p> <p>See also Chapter 34, "Configuring WS-Security".</p>

7. Configure advanced options for the discussion and announcement connection ([Table 14–3](#)).

Table 14–3 Discussion and Announcement Connection - Advanced Configuration

Field	Description
Connection Timeout (in Seconds)	<p>Specify a suitable timeout for the connection.</p> <p>This is the length of time (in seconds) the application waits for a response from the discussions 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>

8. Sometimes, additional parameters are required to connect to the discussions server, for example, those listed in [Table 14–4](#).

Table 14–4 Additional Discussion Connection Properties

Additional Connection Property	Description
<code>application.root.category.id</code>	(WebCenter Portal: Spaces only) Application root category ID on the discussions server under which all discussion forums are stored. For example, if set to 3, then all forums are stored in the category with ID 3.

If additional parameters are required to connect to the discussions server, expand **Additional Properties** and enter details as required (Table 14–5).

Table 14–5 Discussion and Announcement Connection - Additional Properties

Field	Description
Add	<p>Click Add to specify an additional connection parameter:</p> <ul style="list-style-type: none"> ■ Name - Enter the name of the connection property. ■ Value - Enter the default value for the property. ■ Is Property Secured - Indicate whether encryption is required. When selected, the property value is stored securely using encryption. <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 Delete to remove a selected property.</p> <p>Select the correct row before clicking Delete.</p> <p>Note: Deleted rows appear disabled until you click OK.</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 application is deployed. For more information, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

For WebCenter Portal: Spaces, some additional configuration is recommended for the Discussions service. For details, see "Configuring Discussion Forum Options for WebCenter Portal: Spaces" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

14.3.2 Registering Discussions Servers Using WLST

Use the WLST command `createDiscussionForumConnection` to create a discussions server connection. For command syntax and examples, see the section, "createDiscussionForumConnection" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

To configure the Discussions and Announcements services to actively use the new connection, set `default=true`.

Make sure to set additional properties for WS-Security. See [Section 14.5.2, "Modifying Discussions Server Connection Details Using WLST."](#)

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

Note: To start using the new (active) connection you must restart the managed server on which the application is deployed. For more information, see the section, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in *Oracle Fusion Middleware Administrator's Guide*.

14.4 Choosing the Active Connection for Discussions and Announcements

You can register multiple discussions server connections for a WebCenter Portal application, but only one connection is active at a time. The *active connection* becomes the back-end discussions 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 includes the following subsections:

- [Section 14.4.1, "Choosing the Active Connection for Discussions and Announcements Using Fusion Middleware Control"](#)
- [Section 14.4.2, "Choosing the Active Discussion for Discussions and Announcements Using WLST"](#)

14.4.1 Choosing the Active Connection for Discussions and Announcements Using Fusion Middleware Control

To change the active connection:

1. Log in to Fusion Middleware Control and navigate to the home page for the application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
3. From the list of services on the WebCenter Portal 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** checkbox.
6. Click **OK** to update the connection.
7. To start using the new (active) connection you must restart the managed server on which the application is deployed. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

14.4.2 Choosing the Active Discussion for Discussions and Announcements Using WLST

Use the WLST command `setDiscussionForumConnection` with `default=true` to activate an existing connection. For command syntax and examples, see the section,

"setDiscussionForumConnection" in *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. For more information, see the section, "removeDiscussionForumServiceProperty" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

Note: To start using the new (active) connection you must restart the managed server on which the application is deployed. For more information see, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in *Oracle Fusion Middleware Administrator's Guide*.

14.5 Modifying Discussions Server Connection Details

You can modify discussions server connection details at any time.

To start using the modified (active) connection you must restart the managed server on which the application is deployed.

This section includes the following subsections:

- [Section 14.5.1, "Modifying Discussions Server Connection Details Using Fusion Middleware Control"](#)
- [Section 14.5.2, "Modifying Discussions Server Connection Details Using WLST"](#)

14.5.1 Modifying Discussions Server Connection Details Using Fusion Middleware Control

To update connection details for a discussions server:

1. Log in to Fusion Middleware Control and navigate to the home page for the application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
3. From the list of services on the WebCenter Portal 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 14–2](#) and [Table 14–4](#).
6. Click **OK** to save your changes.
7. To start using the updated (active) connection you must restart the managed server on which the application is deployed. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

14.5.2 Modifying Discussions Server Connection Details Using WLST

Use the WLST command `setDiscussionForumConnection` to edit connection details. For command syntax and examples, see the section, "setDiscussionForumConnection" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

To set additional parameters, use the `setDiscussionForumConnectionProperty` command. For more information, see the section, "setDiscussionForumConnectionProperty" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

Note: To start using the updated (active) connection you must restart the managed server on which the application is deployed. For more information, see the section, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in *Oracle Fusion Middleware Administrator's Guide*.

14.6 Deleting Discussions Server Connections

You can delete discussions 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 work, as they all require a back-end discussions server.

This section includes the following subsections:

- [Section 14.6.1, "Deleting a Discussions Server Connection Using Fusion Middleware Control"](#)
- [Section 14.6.2, "Deleting a Discussions Server Connection Using WLST"](#)

14.6.1 Deleting a Discussions Server Connection Using Fusion Middleware Control

To delete a discussions server connection:

1. Log in to Fusion Middleware Control and navigate to the home page for the application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.

3. From the list of services on the WebCenter Portal Services Configuration page, select **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 application is deployed. For more information, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

Note: Before restarting the managed server, mark another connection as active; otherwise, the service is disabled.

14.6.2 Deleting a Discussions Server Connection Using WLST

Use the WLST command `deleteConnection` to remove a connection. For command syntax and examples, see the section, "deleteConnection" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

Ensure that another connection is marked active; otherwise, the service is disabled.

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

Note: To effect this change you must restart the managed server on which the application is deployed. For more information, see the section, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in *Oracle Fusion Middleware Administrator's Guide*.

14.7 Setting Up Discussions Service Defaults

Use the WLST command `setDiscussionForumServiceProperty` to set defaults for the Discussions service in your application:

- `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 Discussions server under which all discussion forums are stored. For example, if set to 3, then all forums are stored in the category with ID 3.
- `ForumGatewayManager.AUTO_START`: Communication through mail distribution lists can be published as discussion forum posts on a Discussions server, as described in "Publishing Space Mail in a Discussion Forum" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*. This parameter starts or stops the gateway for this communication.

For WebCenter Portal: Spaces applications, the default value is 1 (`true`), which means that as soon as you configure mail server settings through administration, the gateway starts. Set this to 0 (`false`), and restart the managed server, to stop the gateway and disable this feature.

For WebCenter Portal: Framework applications, the default value is 0. Set this to 1, and restart the managed server, to start the gateway and enable this feature.

For command syntax and examples, see the section, "setDiscussionForumServiceProperty" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

14.8 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 quick 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 the section, "setAnnouncementServiceProperty" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

14.9 Testing Discussions Server Connections

Try accessing the discussions server with the following URL:

```
http://host:port/owc_discussions
```

You should see a page listing all public information.

14.10 Granting Administrator Permissions on the Discussions Server

The WLST command `addDiscussionsServerAdmin` grants system administrator permissions on the discussions server to a user or a group. This command is useful when you connect the discussions server to a new identity store that does not contain any of the current administrators. For command syntax and examples, see the section, "addDiscussionsServerAdmin" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

14.11 Granting Administrator Role on the Discussions Server

The default domain administrator created for WebCenter Portal is also the administrator for Oracle WebCenter Portal's Discussion Server. You can make a nondefault user the administrator for the discussions server too.

While creating a domain, if you specify any other user as the domain administrator, that user is granted all the domain administrative rights. However, after creating the domain, you must manually grant the administrator role to that nondefault user in both the Spaces application and the discussions server. For information on how to grant administrator privileges to a nondefault user for Spaces, see [Section 30.6.1, "Granting the Spaces Administrator Role."](#)

For Oracle WebCenter Portal's Discussion Server, the default user is the super administrator. This section describes how to grant administrator privileges to a nondefault user.

14.11.1 Granting the Discussions Server Administrator Role using WLST

The WLST command `addDiscussionsServerAdmin` lets you grant system administrator permissions on the Discussions server to a user or a group. This is useful when you connect the discussions server to a new identity store. For command syntax and examples, see the section, "addDiscussionsServerAdmin" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

14.11.2 Granting the Discussions Server Administrator Role using the Admin Console

To grant the administrator role for Oracle WebCenter Portal's Discussion Server to a nondefault user:

1. Log on to the discussions server admin console as an administrator by using the following URL format: `http://host:port/owc_discussions/admin`.
2. Click the **Settings** link in the list of links across the top of the page.
3. Click the **Admins/Moderators** link, if not selected, in the navigation panel on the left.
4. On the Admins & Moderators page, click the **Grant New Permissions** tab.
5. Select the **System Admin** checkbox.
6. Select the **A Specific User** checkbox and specify the user to whom you want to grant administrative privilege for Oracle WebCenter Portal's Discussion Server.
7. Click **Grant New Permission**.

You can now log on to Oracle WebCenter Portal's Discussion Server as the user whom you have assigned the administrative privilege.

Figure 14–3 Granting the Administrator Role on Oracle WebCenter Portal's Discussion Server

Grant New Permissions

Permission Summary | Grant New Permissions

Follow the steps below to grant new user or group permissions: Note, it is not possible to set per Summary page.

- Choose the permissions: [\[select all\]](#)
 - System Admin
 - Category Admin
 - User Admin
 - Group Admin
 - Moderator
- Choose a user or group to grant the permissions to:
 - A Specific User: (enter username - separate multiple usernames with commas)
 - A Specific Group: (enter group name - separate multiple group names with commas)
- Done:

14.11.3 Revoking the Discussions Server Administrator Role

After assigning the discussions server administrator role to the required nondefault user, you may want to revoke the administrator role from the default user.

To revoke the administrator role:

- Log on to discussions server admin console as the nondefault user whom you have assigned the administrator role.
- Click the **Settings** link in the list of links across the top of the page.
- Click the **Admins/Moderators** link, if not selected, in the navigation panel on the left.
- On the Admins & Moderators page, under the **Permission Summary** tab, uncheck the **System Admin** checkbox for the required user, for example, **weblogic**. (Figure 14–4)

Figure 14–4 Revoking the Administrator Role

Permissions Summary

Permission Summary | Grant New Permissions

	System Admin	Category Admin	User Admin	Group Admin	Moderator	Remove
Users						
admin	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
fmwadmin	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
oc4jadmin	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
orcladmin	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
weblogic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Groups						
No group permissions.						
						<input type="button" value="Save Changes"/> <input type="button" value="Cancel"/>

5. Click **Save Changes**.

The administrative privileges for managing Oracle WebCenter Portal's Discussion Server are now revoked from the default user.

14.12 Troubleshooting Issues with Announcements and Discussions

This troubleshooting section includes the following subsections:

- [Section 14.12.1, "Authentication Failed"](#)
- [Section 14.12.2, "Discussions Cannot Be Enabled in a Space"](#)
- [Section 14.12.3, "Login Failed"](#)
- [Section 14.12.4, "Login Does Not Function Properly After Configuring Oracle Access Manager"](#)
- [Section 14.12.5, "Category Not Found Exceptions"](#)

14.12.1 Authentication Failed

Problem

WS-Security does not appear to be set properly for the connection between WebCenter Portal and the back-end discussions server. You may see the following error:

```
failure to authenticate the user WebLogic, due to: Authentication Failed
```

Solution

This error may be caused due to various reasons. Check the following:

- Ensure that the OWSM SAML policy setting is appropriately defined between the discussions connection and the discussions server.
- For the WebCenter Portal Discussions *service*, review `WC_Spaces-diagnostic.log` for errors and exceptions. If the log does not provide enough information to correct errors, then turn on debugging for the `oracle.webcenter.collab.share` and `oracle.webcenter.collab.forum` packages.
- For the back-end discussions *server*, review `WC_Collaboration-diagnostics.log` and `jive.error.log` inside your domain's `$DOMAIN_HOME/config/fmwconfig/servers/SERVER_NAME/owc_discussions/logs` directory. If the logs do not provide enough information to correct errors, then turn on debugging for Oracle WebCenter Portal's Discussion Server. To turn on debug logs, log on to Oracle WebCenter Portal's Discussion Server admin console, go to page logs, the Debug tab, and enable. Restart the `WC_Collaboration` domain to change the logging setting.
- Make sure that the WebCenter Portal application and the back-end discussions server are in time sync. This is important with OWSM WS-Security.

14.12.2 Discussions Cannot Be Enabled in a Space

Problem

Discussions cannot be enabled in any space, even new spaces.

Solution

This error may be caused due to various reasons. Check the following:

- The back-end discussions server is up and running and accessible. See [Section 14.9, "Testing Discussions Server Connections."](#)
- Administrator User Name (`adminUser`) property configured for the active connection has administrative privileges on the application root category (the category configured for WebCenter Portal: Spaces). See [Section 14.3, "Registering Discussions 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 Spaces, that is, the category (on the discussions server) under which all space discussions and announcement are stored.

- Application root category, where all space discussions and announcements are stored, exists on the back-end discussions server.

You can check the application root category ID configured for the Spaces application by navigating to WebCenter Portal Administration, **Configuration**, **Services**, and then **Discussions**. See "Specifying Where Discussions and Announcements are Stored on the Discussions Server" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

14.12.3 Login Failed

Problem

You may see the following login exception:

```
caught exception running task oracle.webcenter.collab.share.LoginFailedException:
failure to authenticate the user monty, due to: Failed to read user monty from
database.
at
oracle.webcenter.collab.forum.internal.jive.JiveAuthenticator.login(JiveAuthentica
tor.java:213)
```

This occurs when an incorrect admin user name is specified.

Solution

Follow these steps:

1. Confirm that the admin user specified while creating the discussion forum connection has access to the Discussions Administration console at `http://host:port/owc_discussions/admin`.
If the user does not have admin privileges, then use the WLST command `addDiscussionsServerAdmin` to provision the user. For more information, see [Section 14.11.1, "Granting the Discussions Server Administrator Role using WLST."](#)
2. Confirm that you have configured the discussion server with the appropriate `DISCUSSIONS` schema. If not, then create or extend the domain using `config.sh` or `was_config.sh`.

14.12.4 Login Does Not Function Properly After Configuring Oracle Access Manager

Problem

When you log in to Oracle WebCenter Portal's Discussion Server after configuring Oracle Access Manager single sign-on, a 500 - Internal Server Error occurs.

Solution

1. If one does not exist, add a user as super admin on Oracle WebCenter Portal's Discussion Server using the WLST command `addDiscussionsServerAdmin`. For command syntax and examples, see the section, "addDiscussionsServerAdmin" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.
2. Log on to the Discussions Admin Console with the super admin account, and navigate to System - System Properties.
3. Create or edit the property `owc_discussions.sso.mode`, and set its value to `true`. For more information, see [Section 31.2.6.2, "Configuring the Discussions Server for SSO."](#)
4. Restart Oracle WebCenter Portal's Discussion Server.

14.12.5 Category Not Found Exceptions

Problem

If you change the connection to use a different discussions server, and if you change the application root category ID from **Administration - Configuration - Services - Discussions**, then you could see exceptions like, "Category Not Found."

Solution

Restart the managed server on which the WebCenter Portal application is deployed.

Managing the Events Service

This chapter describes how to configure and manage the Events service to expose personal Microsoft Exchange calendars in Oracle WebCenter Portal applications.

Always use Fusion Middleware Control or the WLST command-line tool to review and configure back-end services for WebCenter Portal applications. Any changes that you make to WebCenter Portal applications, post deployment, are stored in the MDS metadata store as customizations. See [Section 1.3.5, "WebCenter Portal Configuration Considerations."](#)

Note: Configuration changes for the Events service, through Fusion Middleware Control or using WLST, are not dynamic so you must restart the managed server on which the WebCenter Portal application is deployed for your changes to take effect. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

This chapter includes the following sections:

- [Section 15.1, "What You Should Know About Events Connections"](#)
- [Section 15.2, "Configuration Roadmaps for Personal Events in the Events Service"](#)
- [Section 15.3, "Events Service Prerequisites for Personal Events"](#)
- [Section 15.4, "Registering Events Servers"](#)
- [Section 15.5, "Choosing the Active Events Server Connection"](#)
- [Section 15.6, "Modifying Events Server Connection Details"](#)
- [Section 15.7, "Deleting Event Server Connections"](#)
- [Section 15.8, "Testing Event Server Connections"](#)
- [Section 15.9, "Troubleshooting Issues with Events"](#)

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."](#)

15.1 What You Should Know About Events Connections

In WebCenter Portal: Spaces, the Events service provides space calendars that you can use to schedule meetings, appointments, and any other type of team, project, or group occasion. The Events service also enables you to access your personal Microsoft Exchange calendar, where you can schedule events that are not related to a particular space.

In applications built using WebCenter Portal: Framework, the Events service provides access to your personal Microsoft Exchange calendar only.

Personal calendars are available through a Microsoft Exchange Server; therefore, a connection to that server is required. You can register the Microsoft Exchange Server connection through the Fusion Middleware Control Console or using WLST.

You must mark a connection as active for the service to work. You can register additional Microsoft Exchange Server connections, but only one connection is active at a time.

To view personal events in WebCenter Portal applications, users must have an account on the Microsoft Exchange Server.

15.2 Configuration Roadmaps for Personal Events in the Events Service

Use the roadmaps in this section as an administrator’s guide through the configuration process for providing access to personal events:

- **Roadmap - Configuring Personal Events for WebCenter Portal: Spaces**

The flow chart (Figure 15–1) and table (Table 15–1) in this section provide an overview of the prerequisites and tasks required to get personal events working in WebCenter Portal: Spaces.

Figure 15–1 Configuring Personal Events for WebCenter Portal: Spaces

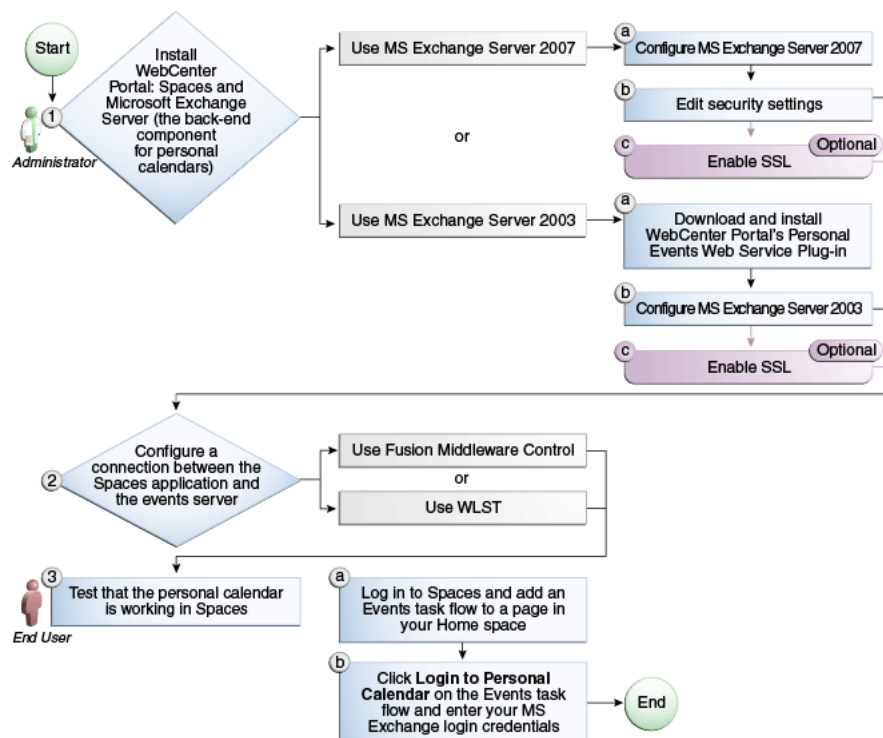


Table 15–1 *Configuring the Personal Events for WebCenter Portal: Spaces*

Actor	Task	Sub-task	Notes
Administrator	1. Install WebCenter Portal: Spaces and Microsoft Exchange Server		MS Exchange Server is the back-end component for personal calendars
	<ul style="list-style-type: none"> ■ Install MS Exchange Server 2007 	1.a Configure MS Exchange Server 2007 1.b Edit security settings 1.c (Optional) Enable SSL	
	<ul style="list-style-type: none"> ■ Install MS Exchange Server 2003 	1.a Download and install WebCenter Portal's Personal Events Web Service Plug-in 1.b Configure MS Exchange Server 2003 1.c (Optional) Enable SSL	
	2. Configure a connection between the Spaces application and the events server using one of the following tools: <ul style="list-style-type: none"> ■ Fusion Middleware Control ■ WLST 		
End User	3. Test that the personal calendar is working in WebCenter Portal: Spaces	3.a Log in to WebCenter Portal: Spaces and add an Events task flow to a page in your Home space 3.b Click Login to Personal Calendar on the Events task flow and enter your MS Exchange Server login credentials	

- **Roadmap - Configuring Personal Events for Framework applications**

The flow chart ([Figure 15–2](#)) and table ([Table 15–2](#)) in this section provide an overview of the prerequisites and tasks required to get personal events working in Framework applications.

Figure 15–2 Configuring Personal Events for Framework applications

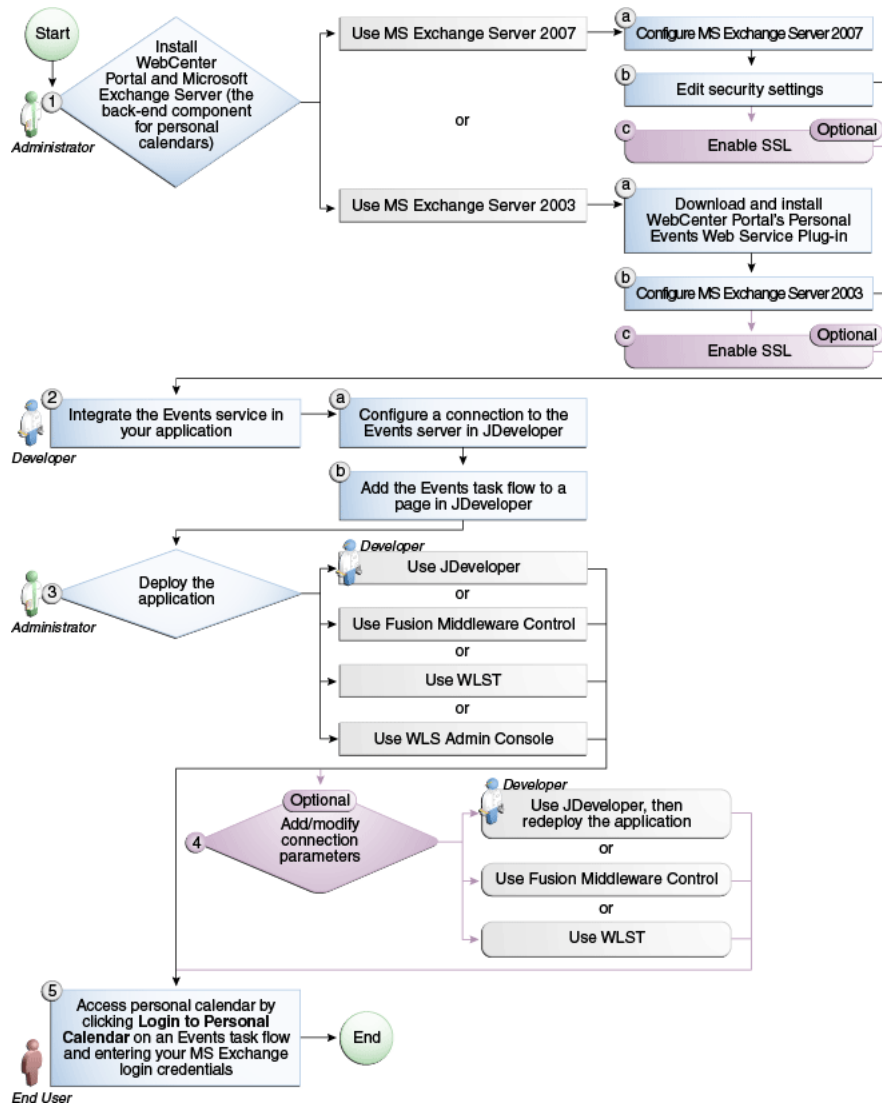


Table 15–2 Configuring Personal Events for Framework applications

Actor	Task	Sub-task	Notes
Administrator	1. Install WebCenter Portal and Microsoft Exchange Server		MS Exchange Server is the back-end component for personal calendars
	<ul style="list-style-type: none"> ■ Use MS Exchange Server 2007 	1.a Configure MS Exchange Server 2007 1.b Edit security settings 1.c (Optional) Enable SSL	
	<ul style="list-style-type: none"> ■ Use MS Exchange Server 2003 	1.a Download and install WebCenter Portal's Personal Events Web Service Plug-in 1.b Configure MS Exchange Server 2003 1.c (Optional) Enable SSL	

Table 15–2 (Cont.) Configuring Personal Events for Framework applications

Actor	Task	Sub-task	Notes
Developer	2. Integrate the Events service in your application	<p>2.a Configure a connection to the events server in JDeveloper</p> <p>2.b Add an Events task flow to a page in JDeveloper</p>	
Developer/ Administrator	<p>3. Deploy the application using one of the following tools:</p> <ul style="list-style-type: none"> ■ JDeveloper (Developer) ■ Fusion Middleware Control (Administrator) ■ WLST (Administrator) ■ WLS Admin Console (Administrator) 		
Developer/ Administrator	<p>4. Add/modify connection parameters using one of the following tools:</p> <ul style="list-style-type: none"> ■ JDeveloper, then redeploy the application (Developer) ■ Fusion Middleware Control (Administrator) ■ WLST (Administrator) 		
End User	5. Click Login to Personal Calendar on the Events task flow and enter your MS Exchange Server login credentials		

15.3 Events Service Prerequisites for Personal Events

This section includes the following subsections:

- [Section 15.3.1, "Microsoft Exchange Server 2007 Prerequisites"](#)
- [Section 15.3.2, "Microsoft Exchange Server 2003 Prerequisites"](#)

15.3.1 Microsoft Exchange Server 2007 Prerequisites

This section describes the Microsoft Exchange Server 2007 prerequisites when used as the server for personal events in the Events service.

This section includes the following subsections:

- [Section 15.3.1.1, "Microsoft Exchange Server 2007 - Installation"](#)
- [Section 15.3.1.2, "Microsoft Exchange Server 2007 - Configuration"](#)
- [Section 15.3.1.3, "Microsoft Exchange Server 2007 - Security Considerations"](#)
- [Section 15.3.1.4, "Microsoft Exchange Server 2007 - Limitations"](#)

15.3.1.1 Microsoft Exchange Server 2007 - Installation

Refer to the Microsoft Exchange Server 2007 documentation for installation information.

15.3.1.2 Microsoft Exchange Server 2007 - Configuration

To use Microsoft Exchange Server 2007 as the server for personal events, you must edit the Microsoft Exchange Server 2007 web service WSDL to specify the location of the web service.

To specify the location of the Microsoft Exchange Server 2007 web service:

1. Open the WSDL file for the Microsoft Exchange Server web service, for example:

```
C:\Program Files\Microsoft\Exchange
Server\ClientAccess\exchweb\ews\Services.wsdl
```

2. Add a service section that points to your Microsoft Exchange Server web service, for example:

```
<wsdl:definitions>
...
  <wsdl:service name="ExchangeServices">
    <wsdl:port name="ExchangeServicePort" binding="tns:ExchangeServiceBinding">
      <soap:address location="https://server.example.com/EWS/Exchange.asmx"/>
    </wsdl:port>
  </wsdl:service>
</wsdl:definitions>
```

15.3.1.3 Microsoft Exchange Server 2007 - Security Considerations

The Events service includes a Microsoft Exchange Server 2007 adapter that communicates with the Microsoft Exchange Server 2007 generic web service through a JAX-WS proxy. To set up the communication between the adapter and the web service, you must edit the Microsoft Exchange Server security settings.

To edit security settings:

1. On the Microsoft Exchange Server, open Internet Information Services (IIS) Manager.
2. Under Node *computer_name* > Web Sites > Default Web Site > EWS, click **Properties**.
3. On the **Directory Security** tab, in the Authentication and access control, click **Edit**.
4. Select **Basic authentication**.
5. Click **OK**.

You must enable anonymous access to *Services.wsdl*, *Messages.vsd*, and *Types.vsd* so that JAX-WS can access them to create the service port before committing any web service call.

6. Right-click **Services.wsdl** and choose **Edit**.
7. On the **File Security** tab, in the Authentication and access control, click **Edit**.
8. Select **Enable anonymous access**.
9. Click **OK**.
10. Repeat steps 6 through 9 for **Messages.xsd** and **Types.xsd**.

The Events service uses Basic Authentication to communicate with the Microsoft Exchange Server. To secure the communication, you should enable SSL. For more information, see:

<http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/56bdf977-14f8-4867-9c51-34c346d48b04.msp?mfr=true>

15.3.1.4 Microsoft Exchange Server 2007 - Limitations

There are currently no known limitations.

15.3.2 Microsoft Exchange Server 2003 Prerequisites

This section describes the Microsoft Exchange Server 2003 prerequisites when used as the server for personal events in the Events service.

This section includes the following subsections:

- [Section 15.3.2.1, "Microsoft Exchange Server 2003 - Installation"](#)
- [Section 15.3.2.2, "Microsoft Exchange Server 2003 - Configuration"](#)
- [Section 15.3.2.3, "Microsoft Exchange Server 2003 - Security Considerations"](#)
- [Section 15.3.2.4, "Microsoft Exchange Server 2003 - Limitations"](#)

15.3.2.1 Microsoft Exchange Server 2003 - Installation

Refer to the Microsoft Exchange Server 2003 documentation for installation information.

15.3.2.2 Microsoft Exchange Server 2003 - Configuration

Microsoft Exchange Server 2003 does not provide a web service, so to use Microsoft Exchange Server 2003 as the server for the Events service, you must install WebCenter Portal's Personal Events Web Service Plug-in on the IIS computer. The plug-in is available on the Oracle Fusion Middleware companion CD.

To install the Personal Events Web Service Plug-in:

1. Extract the contents of `ExchangeWebService.zip` to a folder within the Internet Information Services (IIS) server. You can find the ZIP file in the following directory on the Oracle Fusion Middleware companion CD:

```
/Disk1/WebCenter/services/cal/NT/ExchangeWebService.zip
```

Note: Make sure that the folder where you extract the file has the proper Read privileges. If necessary add Server Operators with additional Modify and Write privileges and Authenticated Users.

2. Open IIS Manager.
3. Under *server_name* > **Web Sites** > **Default Web Site**, create a new virtual directory called `ExchangeWS` (as the **Alias**).
4. Point the new virtual directory to the folder to which you extracted the ZIP file.
5. Make sure the folder has **Read** and **Run Scripts** privileges.
6. Right-click the new virtual directory and choose **Properties**.
7. On the **Virtual Directory** tab, under Application settings, from the **Execute permissions** dropdown list, select **Scripts and Executables**.
8. Click **Apply**.
9. On the **ASP.NET** tab, ensure that the **ASP.NET version** is **2.0.XXXXX**.

Note: If ASP.NET is not available by default, then install the .NET 2.0 Framework from:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=0856eacb-4362-4b0d-8edd-aab15c5e04f5&displaylang=en>

10. Click **Edit Configuration**.

11. In the ASP .NET Configuration Settings dialog, make sure the **ExchangeServerURL** has the correct value, for example:

`http://localhost:port/Exchange/User/calendar`

Tip: The **ExchangeServerURL** is case-sensitive.

Change the port, if necessary, to reflect the IIS port number. By default, this is 80.

12. Apply the changes and close the dialog.

13. Create a folder called `C:\WSErrorLogs`.

14. Test the web service from the IIS server and the WebCenter Portal server by accessing the following URL in your browser:

`http://host:port/ExchangeWS/PersonalEventsWebService.asmx`

15.3.2.3 Microsoft Exchange Server 2003 - Security Considerations

The Events service uses Basic Authentication to communicate with the Microsoft Exchange Server. To secure the communication, you should enable SSL. For more information, see:

<http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/56bdf977-14f8-4867-9c51-34c346d48b04.msp?mfr=true>

15.3.2.4 Microsoft Exchange Server 2003 - Limitations

There are currently no known limitations.

15.4 Registering Events Servers

You can register multiple events servers for a WebCenter Portal application but only one is active at a time.

To start using a new (active) connection you must restart the managed server on which the application is deployed.

This section includes the following subsections:

- [Section 15.4.1, "Registering Events Servers Using Fusion Middleware Control"](#)
- [Section 15.4.2, "Registering Event Servers Using WLST"](#)

15.4.1 Registering Events Servers Using Fusion Middleware Control

To register an events server:

1. Log in to Fusion Middleware Control and navigate to the home page for the WebCenter Portal application. For more information, see:

- [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:
 - For Spaces applications - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
 3. From the list of services on the WebCenter Portal Service Configuration page, select **Personal Events**.
 4. To connect to a new events server instance, click **Add** ([Figure 15-3](#)).

Figure 15-3 Configuring Events Connections

5. Enter a unique name for this connection, specify the version of Microsoft Exchange Server, and indicate whether this connection is the active (or default) connection for the application ([Table 15-3](#)).

Table 15-3 Personal Events Connection - Name

Field	Description
Connection Name	Enter a unique name for the connection. The name must be unique (across all connection types) within the WebCenter Portal application.
Connection Type	Choose the Microsoft Exchange Server you want to connect to: <ul style="list-style-type: none"> ■ Microsoft Exchange Server 2003 ■ Microsoft Exchange Server 2007
Active Connection	Select to use this connection for the Events service in the WebCenter Portal application. While you can register multiple events server connections, only one connection is used by the Events service—the default (or active) connection.

6. Enter connection details for the events server ([Table 15-4](#)).

Table 15–4 Personal Events - Connection Details

Field	Description
Web Service URL	<p>Enter the URL of the web service exposing the event application.</p> <p>Use the format:</p> <pre>protocol://host:port/appWebServiceInterface/WSName</pre> <p>For example</p> <pre>http://myexchange.com:80/ExchangeWS/PersonalEventsWebService.asmx</pre> <pre>http://myexchange.com:80/EWS/Services.wsdl</pre>
Associated External Application	<p>Associate the events service with an external application. External application credential information is used to authenticate users against the Microsoft Exchange Server hosting events services.</p>

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 Portal application is deployed. For more information, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

15.4.2 Registering Event Servers Using WLST

Use the WLST command `createPersonalEventConnection` to create an events server connection. Use `setPersonalEventConnection` to alter an existing connection. For command syntax and examples, see the sections, “`createPersonalEventConnection`” and “`setPersonalEventConnection`” in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.13.3.1, "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 Portal application is deployed. See, “Starting and Stopping WebLogic Managed Servers Using the Command Line” in the *Oracle Fusion Middleware Administrator’s Guide*.

15.5 Choosing the Active Events Server Connection

You can register multiple events server connections with a WebCenter Portal application, but only one connection is active at a time.

This section includes the following subsections:

- [Section 15.5.1, "Choosing the Active Events Server Using Fusion Middleware Control"](#)
- [Section 15.5.2, "Choosing the Active Events Server Connection Using WLST"](#)

15.5.1 Choosing the Active Events Server Using Fusion Middleware Control

To change the active connection:

1. Log in to Fusion Middleware Control and navigate to the home page for the WebCenter Portal application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:
 - For Spaces applications - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
3. From the list of services on the WebCenter Portal Services Configuration page, select **Personal Events**.
The Manage Personal Events 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** checkbox.
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 Portal application is deployed. For more information, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

15.5.2 Choosing the Active Events Server Connection Using WLST

Use the WLST command `setPersonalEventConnection` with `default=true` to activate an existing events server connection. For command syntax and examples, see the section, "setPersonalEventConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

To subsequently disable an events 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 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

Note: To start using the active connection you must restart the managed server on which the WebCenter Portal application is deployed. For more information, see the section, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

15.6 Modifying Events Server Connection Details

You can modify events server connection details at any time.

To start using the updated (active) connection you must restart the managed server on which the WebCenter Portal application is deployed.

This section includes the following subsections:

- [Section 15.6.1, "Modifying Events Server Connection Details Using Fusion Middleware Control"](#)
- [Section 15.6.2, "Modifying Events Server Connection Details Using WLST"](#)

15.6.1 Modifying Events Server Connection Details Using Fusion Middleware Control

To update connection details for an events server:

1. Log in to Fusion Middleware Control and navigate to the home page for the WebCenter Portal application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:
 - For Spaces applications - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
3. From the list of services on the WebCenter Portal Service Configuration page, select **Personal Events**.
4. Select the connection name, and click **Edit**.
5. Edit connection details, as required. For detailed parameter information, see [Table 15-4](#).
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 Portal application is deployed. For more information, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

15.6.2 Modifying Events Server Connection Details Using WLST

Use the WLST command `setPersonalEventConnection` to edit an existing events server connection. For command syntax and examples, see the section, "`setPersonalEventConnection`" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.13.3.1, "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 Portal application is deployed. For more information, see the section, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

15.7 Deleting Event Server Connections

You can delete events server connections at any time but take care when deleting the active connection. If you delete the active connection, users cannot create events in their personal calendar.

This section includes the following subsections:

- [Section 15.7.1, "Deleting Event Server Connections Using Fusion Middleware Control"](#)
- [Section 15.7.2, "Deleting Event Server Connections Using WLST"](#)

15.7.1 Deleting Event Server Connections Using Fusion Middleware Control

To delete an events server connection:

1. Log in to Fusion Middleware Control and navigate to the home page for the WebCenter Portal application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:
 - For Spaces applications - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
3. From list of services on the WebCenter Portal Service Configuration page, select **Personal Events**.
4. Select the connection name, and click **Delete**.
5. To effect this change you must restart the managed server on which the WebCenter Portal application is deployed. For more information, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

15.7.2 Deleting Event Server Connections Using WLST

Use the WLST command `deleteConnection` to remove an events server connection. For command syntax and examples, see the section, "deleteConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

Note: To effect this change you must restart the managed server on which the WebCenter Portal application is deployed. For more information, see the section, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

15.8 Testing Event Server Connections

To confirm the connection to the events server:

1. Add the Events task flow to a page in your WebCenter Portal application.

Tip: In WebCenter Portal: Spaces, add the task flow to a page in your Home space.

2. Log in to your Microsoft Exchange Server account.

3. Your personal events from Microsoft Exchange Server should display in the task flow.

15.9 Troubleshooting Issues with Events

If users cannot see their personal events, verify the following:

- Is the Microsoft Exchange Server/IIS server accessible from the managed server on which the WebCenter Portal application is deployed? Can they ping each other?
- Is the configuration correct on the Microsoft Exchange Server? For more information, see [Section 15.3.1.2, "Microsoft Exchange Server 2007 - Configuration"](#) or [Section 15.3.2.2, "Microsoft Exchange Server 2003 - Configuration."](#)
- Is the events server connection correct in the managed server? For more information, see [Section 15.4, "Registering Events Servers."](#)
- Did the user enter the correct user name and password for the account on the Microsoft Exchange Server? The user name is usually an email address.

Managing the Instant Messaging and Presence Service

This chapter describes how to configure and manage the Instant Messaging and Presence (IMP) service for your WebCenter Portal application.

Always use Fusion Middleware Control or WLST command-line tool to review and configure back-end services for WebCenter Portal applications. Any changes that you make to your applications, post deployment, are stored in MDS metadata store as customizations. See [Section 1.3.5, "WebCenter Portal Configuration Considerations."](#)

Note: Configuration changes for the Instant Messaging and Presence service, through Fusion Middleware Control or using WLST, are not dynamic so you must restart the managed server on which your application is deployed for changes to take effect. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

This chapter includes the following sections:

- [Section 16.1, "What You Should Know About Instant Messaging and Presence Connections"](#)
- [Section 16.2, "Instant Messaging and Presence Server Prerequisites"](#)
- [Section 16.3, "Registering Instant Messaging and Presence Servers"](#)
- [Section 16.4, "Choosing the Active Connection for Instant Messaging and Presence"](#)
- [Section 16.5, "Modifying Instant Messaging and Presence Connection Details"](#)
- [Section 16.6, "Deleting Instant Messaging and Presence Connections"](#)
- [Section 16.7, "Setting Up Instant Messaging and Presence Service Defaults"](#)
- [Section 16.8, "Testing Instant Messaging and Presence 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."](#)

16.1 What You Should Know About Instant Messaging and Presence Connections

The IMP service enables you to observe the presence status of other authenticated application users (online, offline, busy, or away) and provides instant access to interaction options, such as instant messages (IM) and mails.

A single connection to a back-end presence server is required. WebCenter Portal is certified with Microsoft Office Live Communications Server (LCS) 2005, Microsoft Office Communications Server (OCS) 2007, and Microsoft Lync 2010.

Notes: Oracle Beehive Server connections are not supported in this release.

You can register the presence server connection for your application through the Fusion Middleware Control Console or 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.

16.2 Instant Messaging and Presence Server Prerequisites

This section includes the following subsections:

- [Section 16.2.1, "Microsoft Live Communications Server \(LCS\) Prerequisites"](#)
- [Section 16.2.2, "Microsoft Office Communications Server \(OCS\) Prerequisites"](#)
- [Section 16.2.3, "Microsoft Lync Prerequisites"](#)

16.2.1 Microsoft Live Communications Server (LCS) Prerequisites

This section describes the Microsoft Live Communications Server 2005 (LCS) prerequisites as the presence server for the Instant Messaging and Presence service.

This section includes the following subsections:

- [Section 16.2.1.1, "Microsoft LCS - Installation"](#)
- [Section 16.2.1.2, "Microsoft LCS - Configuration"](#)
- [Section 16.2.1.3, "Microsoft LCS - Security Considerations"](#)

16.2.1.1 Microsoft LCS - Installation

Refer to the Microsoft Live Communications Server 2005 documentation for installation information.

16.2.1.2 Microsoft LCS - Configuration

To use Microsoft Live Communications Server 2005 as the presence server for the Instant Messaging and Presence service, you must install and configure the Microsoft RTC API v1.3, and you must install the Oracle RTC Web service for Microsoft LCS 2005.

1. To install the Microsoft RTC API v1.3, download the RTC SDK from Microsoft RTC Client API SDK 1.3, and run the installer. The installer provides the necessary installation components. If you choose the default options, the following two installers are available at `C:\Program Files\RTC Client API v1.3 SDK\INSTALLATION:`

- RtcApiSetup.msi
- RtcSxSPolicies.msi

Run the `RtcApiSetup.msi` installer first, then the side-by-side policy switcher installer (`RtcSxSPolicies.msi`), and restart the system.

2. To install the Oracle RTC Web service for Microsoft Live Communications Server 2005, extract the `owc_lcs.zip` file from the Oracle Fusion Middleware companion CD. It is located in the directory `/Disk1/WebCenter/services/imp/NT`. The zip file contains the following:

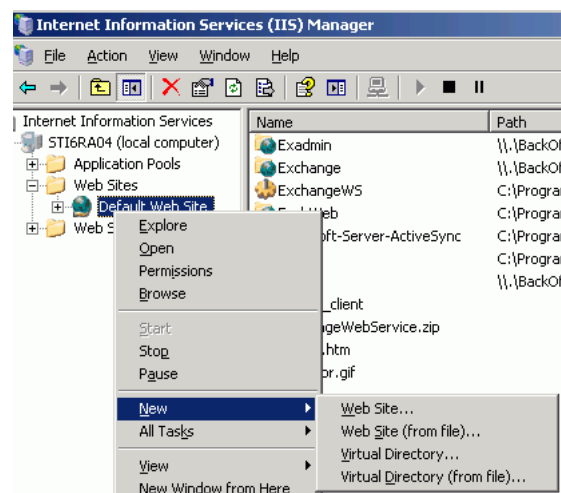
```

/Bin
/images
ApplicationConfigurationService.asmx
BlafPlus.css
ExtAppLogin.aspx
ExtAppLogin.aspx.cs
Global.asax
Log4Net.config
RTCService.asmx
Web.Config
WebcenterTemplate.master

```

3. Open the Internet Information Services (IIS) Manager.
4. Expand the server node and then **Web Sites** in the IIS Manager window.
5. Right-click **Default Web Site**, choose **New**, and then select **Virtual Directory** to create a site for the Oracle RTC Web service, as shown in [Figure 16-1](#). The Virtual Directory Creation Wizard displays.

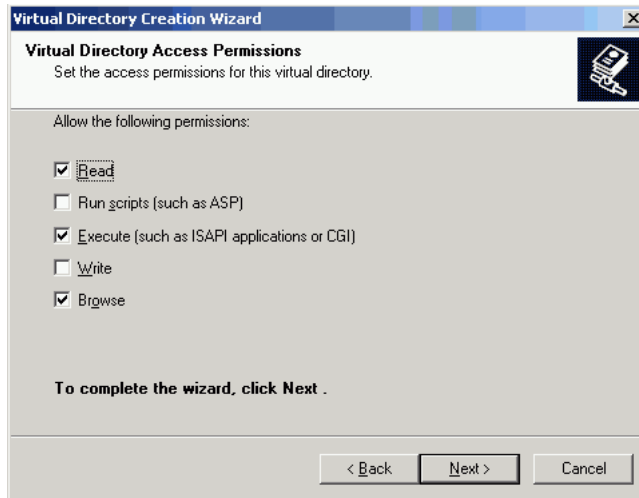
Figure 16-1 *Creating a Virtual Directory*



6. Click **Next**.
7. Enter an alias for the virtual directory in the **Alias** field, for example **RTC**.

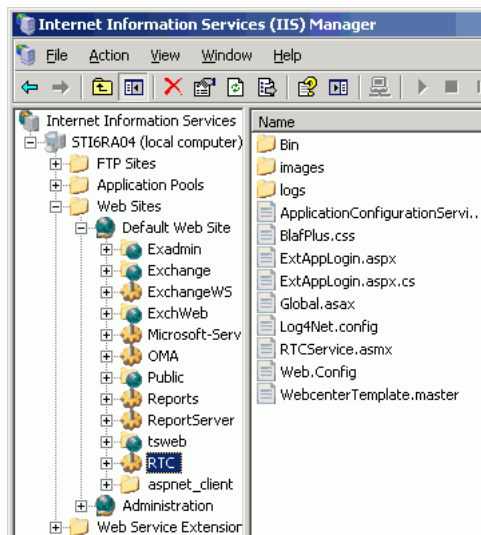
8. Enter the path to the directory where you extracted the `owc_1cs.zip` file. Alternatively, use the **Browse** button to navigate to that directory.
9. Click **Next**.
10. Ensure that the virtual directory has the Read, Execute, and Browse privileges. (Figure 16–2)

Figure 16–2 Virtual Directory Properties



11. Click **Next**.
12. Click **Finish**. The newly created virtual directory appears under **Default Web Site** in the Internet Information Services (IIS) Manager window (Figure 16–3).

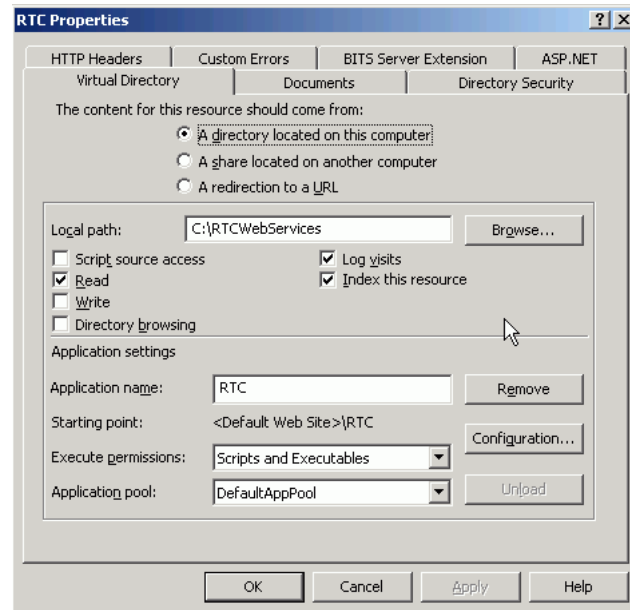
Figure 16–3 Adding a Virtual Directory



13. Right-click the newly created virtual directory for the Oracle RTC Web service, and then choose **Properties** to open the Properties dialog.
14. 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.

15. Select **Scripts and Executables** from the **Execute permissions** dropdown list (Figure 16–4).

Figure 16–4 Virtual Directory Properties



16. 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.
17. Click **OK**.
18. Ensure that the LSC pool name in the LCS connection has been set.
19. 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
```

16.2.1.3 Microsoft 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 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.

For more information, see [Section 16.3.1, "Registering Instant Messaging and Presence Servers Using Fusion Middleware Control."](#)

16.2.2 Microsoft Office Communications Server (OCS) Prerequisites

This section describes the Microsoft Office Communications Server 2007 (OCS) prerequisites as the presence server for the Instant Messaging and Presence service.

This section includes the following subsections:

- [Section 16.2.2.1, "Microsoft OCS - Installation"](#)
- [Section 16.2.2.2, "Microsoft OCS - Configuration"](#)
- [Section 16.2.2.3, "Microsoft OCS - Security Considerations"](#)

16.2.2.1 Microsoft OCS - Installation

Refer to the Microsoft Office Communications Server 2007 documentation for installation information.

16.2.2.2 Microsoft OCS - Configuration

To use Microsoft OCS 2007 as the presence server for the IMP service, you must deploy WebCenter Portal's Proxy application for Microsoft OCS 2007 in one of two topologies:

- [Simple Deployment](#) – All components reside on the same box
- [Remote Deployment](#) – The proxy application and Microsoft OCS reside on separate boxes

16.2.2.2.1 Simple Deployment In this topology, WebCenter Portal's Proxy application is deployed in the Internet Information Services (IIS) server hosted on the OCS box.

1. Install Microsoft Unified Communications Managed API (UCMA) 2.0 on the OCS box.

For detailed information, see [Section 16.2.2.2.6, "Installing UCMA v2.0."](#)

2. Deploy WebCenter Portal's Proxy application on the IIS server. This proxy application provides web services for interacting with the OCS server and sending/receiving information. WebCenter Portal talks to these web services and presents the data.

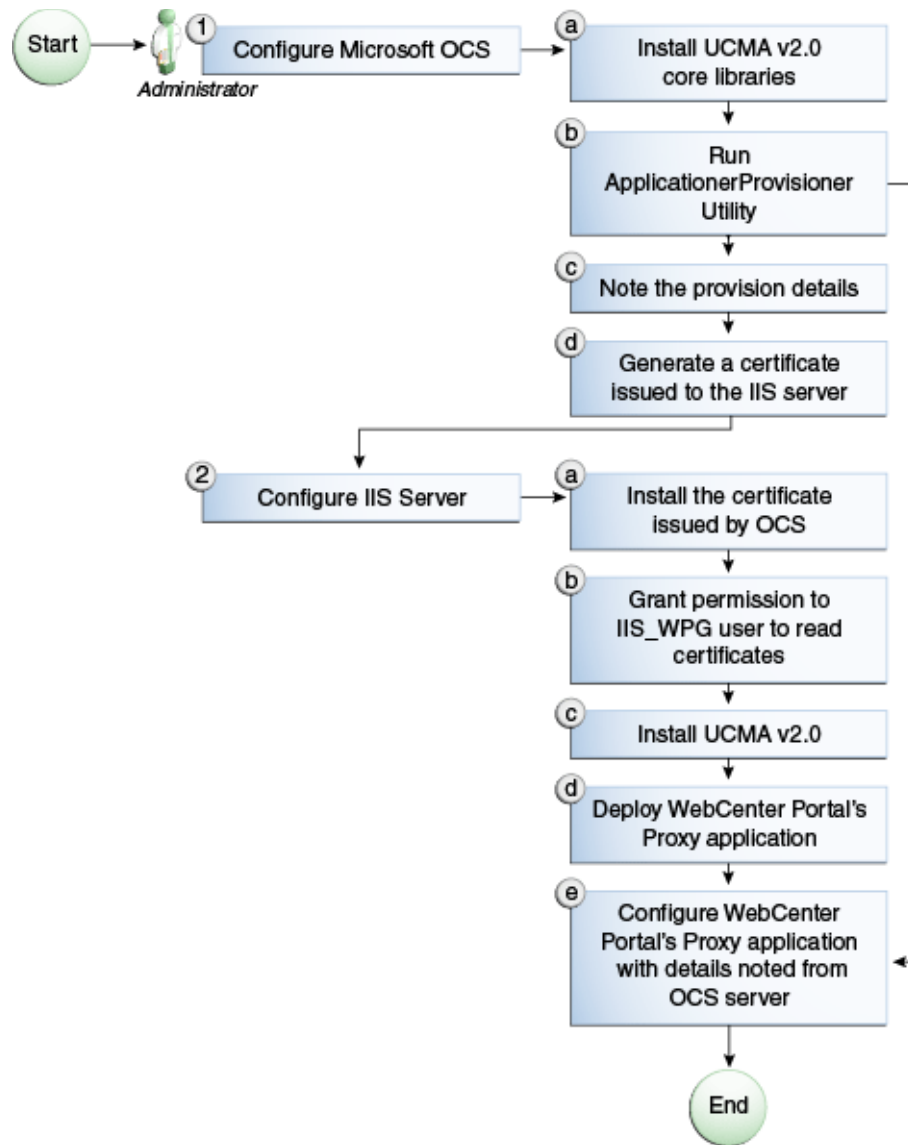
For detailed information, see [Section 16.2.2.2.7, "Installing WebCenter Portal's Proxy Application."](#)

16.2.2.2.2 Remote Deployment In this topology, WebCenter Portal's Proxy application is deployed on an IIS server remote to the OCS box. That is, the IIS server and the OCS server are hosted on separate machines.

Because this proxy application is hosted on a remote box, you must set up a trust between the application and the OCS server. This is known as provisioning an application. Provisioning is done through the Application Provisioner utility shipped with Microsoft UCMA v2.0. For more details, see <http://msdn.microsoft.com/en-us/library/dd253360%28office.13%29.aspx>.

[Figure 16–5](#) provides an overview of the steps (including installing UCMA v2.0) to be performed on different deployment entities.

Figure 16-5 Microsoft OCS Configuration - Remote Deployment



The details of these steps are described in the following sections.

16.2.2.2.3 Building Application Provisioner This section lists the steps Microsoft provides for provisioning other IIS servers to access OCS.

1. Install Visual Studio 2008 on any developer box (not necessarily IIS/OCS).
2. Install UCMA version 2.0 on the same box following the steps in [Section 16.2.2.2.6, "Installing UCMA v2.0."](#) The Application Provisioner application comes with the UCMA SDK.
3. Go to the directory `Sample Applications\Collaboration\ApplicationProvisioner` under the location where you installed UCMA Core (for example, `C:\Program Files\Microsoft Office Communications Server 2007 R2\UCMA SDK 2.0\UCMACore\Sample Applications\Collaboration\ApplicationProvisioner`).

4. The directory contains the Application Provisioner application. Build the application using Visual Studio 2008. This generates the `ApplicationProvisioner.exe` file.
5. Copy the executable file to the OCS box.

16.2.2.2.4 Provisioning WebCenter Portal's Proxy Application on OCS Server

1. Install UCMA v2.0 core libraries on the OCS box. Follow the same steps in [Section 16.2.2.2.6, "Installing UCMA v2.0,"](#) except that after installing Visual C++ 2008 Redistributable, run `OCSCore.msi`. This installs the WMI classes required to provision an application.
2. Run the `ApplicationProvisioner.exe` file, generated in the previous section. This launches the Application Provisioner dialog.
3. In the Application Provisioner dialog, enter `WebCenterProxyApplication` as the name of your application for the Application name, and then click **Find or Create**.
4. In the Create Application Pool dialog, select the Office Communications Server pool for your application in the OCS Pool Fqdn list. For Listening port, enter the listening port for your application (for example, 6001). For Application server Fqdn, enter the fully qualified domain name (FQDN) of the computer on which the application is deployed. (This is the IIS box.)

If the application is deployed on two or more computers, then select the Load balanced application checkbox, and for Load balancer Fqdn, enter the FQDN of the load balancer.

5. The application pool now appears in the Application Provisioner dialog. Double-click the server entry. The View Server dialog appears. Note the information shown there; that is, Server FQDN, port, and GRUU.
6. Create a certificate on the OCS server with the subject name as the Server FQDN noted in the previous step using the Office Communications Server Certificate Wizard. This certificate is used to authorize the requests coming from the IIS server.
7. After the certificate is created, view the certificate. On the Details tab click **Copy to File**. This launches the Certificate Export Wizard. Export the certificate with the private key to a file. This creates a .pfx (Personal Information Exchange) file with the certificate name.

16.2.2.2.5 IIS Server Configuration Because the IIS server hosts WebCenter Portal's Proxy application in the remote deployment scenario, use the information from the previous section to make it a trusted authority.

1. Install the certificate issued by the OCS server with the private key: Copy the .pfx file generated in step 7 under section "[Provisioning WebCenter Portal's Proxy Application on OCS Server](#)" to the IIS box, and double-click it. This launches the Certificate Import wizard. Import the certificate in Personal Folder under LOCAL_MACHINE.
2. Give permission to IIS_WPG user for reading the certificate. This is required so that the IIS server has appropriate read access on the certificate. This could be done using a utility provided by Microsoft called Windows HTTP Services Certificate Configuration Tool (<http://www.microsoft.com/downloads/details.aspx?familyid=c42e27ac-3409-40e9-8667-c748e422833f&displaylang=en>). Download the

utility and install it. This creates an executable called `winhttpcertcfg.exe`. Go to the install location and run the following command to grant permission:

```
winhttpcertcfg.exe -g -c LOCAL_MACHINE\MY -s "<certificate-name>" -a "IIS_WPG"
```

3. Make an entry in `C:/WINDOWS/system32/drivers/etc/hosts` for the pool name of the OCS server as follows:

```
<ip-address-of-ocs-box> <poolname-of-ocs-box>
```

For example:

```
10.177.252.146 pool101.example.com
```

4. Because the IIS server hosts WebCenter Portal's Proxy application, install Microsoft UCMA v2.0 on it.

For detailed information, see [Section 16.2.2.2.6, "Installing UCMA v2.0."](#)

5. After UCMA is installed, deploy the proxy application on the IIS server. WebCenter Portal's Proxy application provides web services for interacting with OCS server and sending/receiving information. WebCenter Portal talks to these web services and presents the data.

For detailed information, see [Section 16.2.2.2.7, "Installing WebCenter Portal's Proxy Application."](#)

6. Go to the location where WebCenter Portal's Proxy application was extracted. Open `Web.config` and edit the `appSettings` XML node to add the values noted in Step 7 in previous section. Ensure to set value for `RemoteDeployment` to `true`.

For example, the `appSettings` XML node should look somewhat like this.

```
<appSettings>
  <add key="ApplicationName" value="WebCenterProxyApplication" />
  <add key="RemoteDeployment" value="true" />
  <add key="ApplicationFQDN" value="iis.server.com" />
  <add key="ApplicationGRUU"
value="sip:iis.server.com@EXAMPLE.COM;gruu;opaque=srvr:WebCenterProxyApplicatio
n:7mhSo94PLUK-5Q2bKPLyMAAA" />
  <add key="ApplicationPort" value="6001" />
</appSettings>
```

The trust is established, and WebCenter Portal's Proxy application can talk to OCS.

16.2.2.2.6 Installing UCMA v2.0 Microsoft Unified Communications Managed API v2.0 (UCMA) is an endpoint API that allows advanced developers to build server applications that can interact with the OCS environment.

In a simple deployment, the UCMA is installed on the same box as OCS. In a remote deployment, the OCS core libraries are installed on the OCS box, and the UCMA is installed on the IIS (proxy) box.

1. Download UCMA v2.0 from the following location:

- For OCS2007 R1 installation (32 bit):
<http://www.microsoft.com/downloads/details.aspx?FamilyID=768efa33-6606-4b2b-809a-6c69274621d3&displaylang=en>

Download and run the `UcmaSDKWebDownload.msi` file. This extracts set up files to the folder `C:\Microsoft Unified Communications Managed API 2.0 SDK Installer package\i386`.

- For OCS2007 R2 installation (64 bit):
<http://www.microsoft.com/downloads/details.aspx?FamilyID=b20967b1-6cf5-4a4b-b7ae-622653ac929f&displaylang=en>

Download and run the `UcmaSDKWebDownload.msi` file. This extracts set up files to the folder `C:\Microsoft Unified Communications Managed API 2.0 SDK Installer package\amd64`.

2. Go to the directory (where the files from the previous step were extracted) and run `vcredist_x86.exe`. This installs run-time components of Visual C++ Libraries required for UCMA APIs. Go to directory called `Setup` and run `UcmaRedist.msi`. This installs the UCMA 2.0 assemblies in the GAC.

16.2.2.2.7 Installing WebCenter Portal's Proxy Application

1. Extract `owc_ocs2007.zip` from the companion CD. This creates a directory named `OCSWebServices`.
2. Open the Internet Information Services (IIS) Manager.
3. Expand the server node and then **Web Sites** in the Internet Information Services (IIS) Manager.
4. Right-click **Default Web Site**, choose **New**, and then select **Virtual Directory** to create a site for the Oracle RTC Web service. The Virtual Directory Creation Wizard displays. Click **Next**.
5. Enter an alias for the virtual directory in the **Alias** field, for example `RTC`.
6. Enter the path to the directory extracted from `owc_ocs2007.zip` file. If you had extracted the zip file in `C:\`, then the path supplied should be `C:\OCSWebServices`. Alternatively, use the **Browse** button to navigate to that directory. Click **Next**.
7. Ensure that the virtual directory has the **Read**, **Execute**, and **Browse** privileges. Click **Next**.
8. Click **Finish**. The newly created virtual directory appears under **Default Web Site** in the Internet Information Services (IIS) Manager window.
9. Right-click the newly created virtual directory for the Oracle RTC Web service, and then choose **Properties** to open the Properties dialog.
10. 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.
11. Select **Scripts and Executables** from the **Execute permissions** dropdown list.
12. 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. Click **OK**.
13. Test the Web service by accessing the Web site from the following URL format:
`http://localhost/default_website/OCSWebService.asmx`

where `default_website` is the virtual directory you created for the Oracle RTC Web service

For example:

`http://localhost/RTC/OCSWebService.asmx`

16.2.2.3 Microsoft OCS - Security Considerations

You must configure an external application for Microsoft Office Communications Server connections so that users can supply credentials to authenticate themselves on the OCS server.

With a secured application, users get presence status. With OCS, if security is required, then OCS should be on a private trusted network.

OCS 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.

For more information, see [Section 16.3.1, "Registering Instant Messaging and Presence Servers Using Fusion Middleware Control."](#)

16.2.3 Microsoft Lync Prerequisites

This section describes the Microsoft Lync 2010 prerequisites as the presence server for the Instant Messaging and Presence service.

This section includes the following subsections:

- [Section 16.2.3.1, "Microsoft Lync - Installation"](#)
- [Section 16.2.3.2, "Microsoft Lync - Configuration"](#)
- [Section 16.2.3.3, "Microsoft Lync - Security Considerations"](#)

16.2.3.1 Microsoft Lync - Installation

Refer to the Microsoft Lync 2010 documentation for installation information.

16.2.3.2 Microsoft Lync - Configuration

Configuration for Microsoft Lync is similar to configuration for Microsoft OCS.

To use Microsoft Lync 2010 as the presence server for the IMP service, you must deploy WebCenter Portal's Proxy application for Microsoft Lync 2010 in one of two topologies:

- [Simple Deployment](#) – All components reside on the same box
- [Remote Deployment](#) – The proxy application and Microsoft Lync reside on separate boxes

16.2.3.2.1 Simple Deployment In this topology, WebCenter Portal's Proxy application is deployed in the Internet Information Services (IIS) server hosted on the Lync box.

1. Install Microsoft Unified Communications Managed API (UCMA) 2.0 on the Lync box.

For detailed information, see [Section 16.2.3.2.8, "Installing UCMA v2.0."](#)

2. Deploy WebCenter Portal's Proxy application on the IIS server. This proxy application provides web services for interacting with the Lync server and sending/receiving information. WebCenter Portal talks to these web services and presents the data.

For detailed information, see [Section 16.2.3.2.9, "Installing WebCenter Portal's Proxy Application."](#)

16.2.3.2.2 Remote Deployment In this topology, WebCenter Portal's Proxy application is deployed on an IIS server remote to the Lync box. That is, the IIS server and the Lync server are hosted on separate machines.

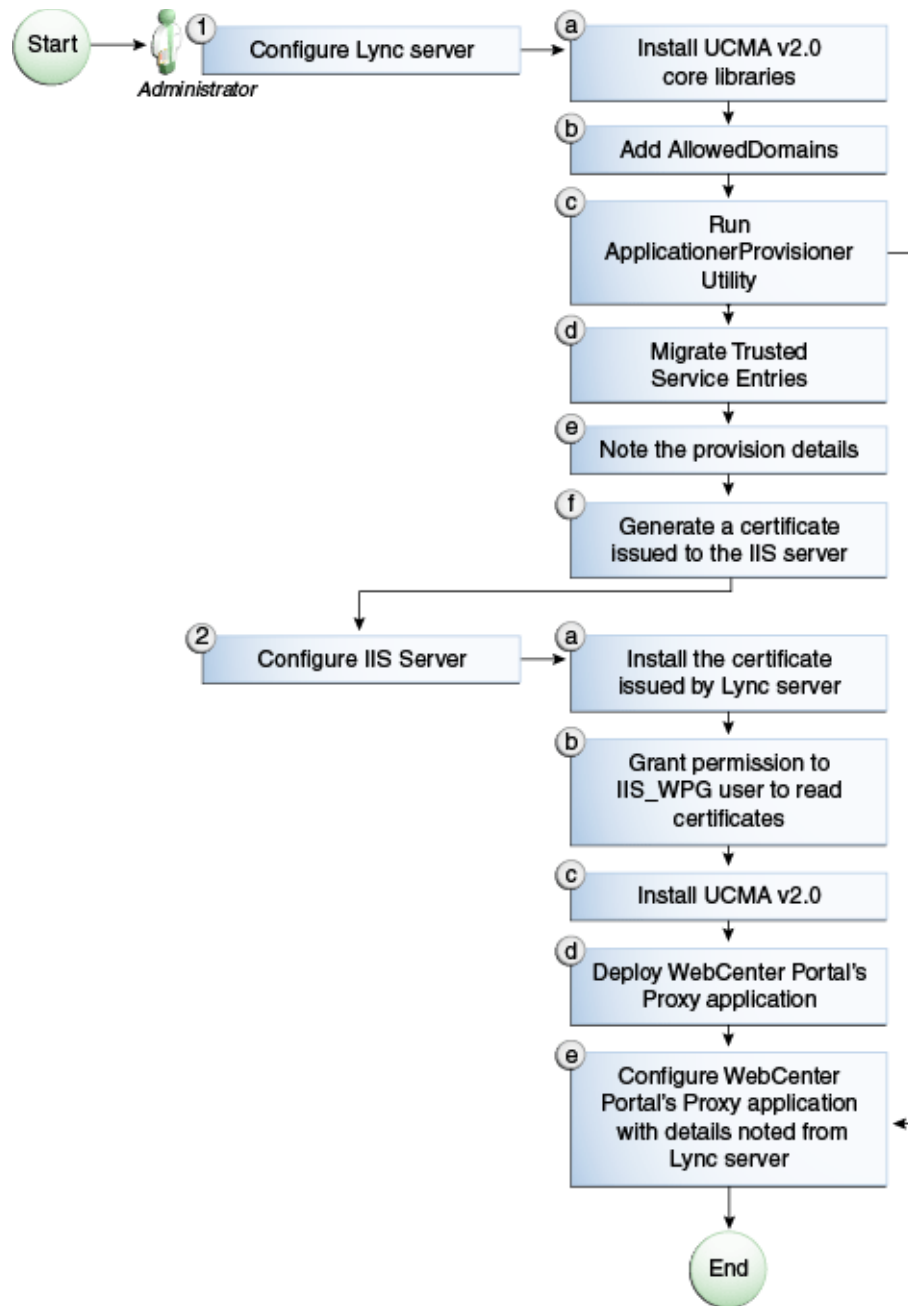
Because this proxy application is hosted on a remote box, you must set up a trust between the application and the Lync server. This is known as provisioning an application. Provisioning is done through the Application Provisioner utility shipped with Microsoft UCMA v2.0.

See Also:

<http://msdn.microsoft.com/en-us/library/dd253360%28office.13%29.aspx>

Figure 16–6 provides an overview of the steps (including installing UCMA v2.0) to be performed on different deployment entities.

Figure 16–6 Microsoft Lync Configuration - Remote Deployment



The details of these steps are described in the following sections.

16.2.3.2.3 Building Application Provisioner This section lists the steps Microsoft provides for provisioning other IIS servers to access Lync.

1. Install Visual Studio 2008 on any developer box (not necessarily IIS/Lync).
2. Install UCMA version 2.0 on the same box following the steps in [Section 16.2.3.2.8, "Installing UCMA v2.0."](#) The Application Provisioner application comes with the UCMA SDK.
3. Go to the directory `Sample Applications\Collaboration\ApplicationProvisioner` under the

location where you installed UCMA Core (for example, `C:\Program Files\Microsoft Lync 2010 R2\UCMA SDK 2.0\UCMACore\Sample Applications\Collaboration\ApplicationProvisioner`).

4. Open the application in Visual Studio 2008 and edit the `Application.cs` file as per <http://msdn.microsoft.com/en-us/library/gg448038.aspx>.
5. Build the application using Visual Studio 2008. This generates the `ApplicationProvisioner.exe` file.
6. Copy the executable file to the Lync box.

16.2.3.2.4 Provisioning WebCenter Portal's Proxy Application on Lync Server

1. Run the `OCSWMIBC.msi` file that comes with the Lync setup package.
2. When a UCMA 2.0 application is deployed directly against Lync Server 2010, the SIP domains used in the Lync Server 2010 environment must be added to the Office Communications Server 2007 R2 SIP domain list *before* you run the `Merge-CsLegacyTopology` cmdlet. The application is deployed as if it were being deployed against OCS 2007 R2, then migrated to run against Lync Server 2010. To add the domains, see [Section 16.2.3.2.5, "Adding AllowedDomains Using WBemTest."](#)
3. Run the `ApplicationProvisioner.exe` file, generated in the previous section. This launches the Application Provisioner dialog.
4. In the Application Provisioner dialog, enter `WebCenterProxyApplication` as the name of your application for the Application name, and then click **Find or Create**.
5. In the Create Application Pool dialog, select the pool for your application in the Lync Pool Fqdn list. For Listening port, enter the listening port for your application (for example, 6001). For Application server Fqdn, enter the fully qualified domain name (FQDN) of the computer on which the application is deployed. (This is the IIS box.)

If the application is deployed on two or more computers, then select the Load balanced application checkbox, and for Load balancer Fqdn, enter the FQDN of the load balancer.

6. The application pool now appears in the Application Provisioner dialog. Double-click the server entry. The View Server dialog appears. Note the information shown there; that is, Server FQDN, port, and GRUU.
7. The newly-created trusted entry must be migrated to Lync Server 2010. See [Section 16.2.3.2.6, "Migrating Trusted Service Entries Using Topology Builder or PowerShell Cmdlets."](#)
8. Create a certificate on the Lync server with the subject name as the Server FQDN noted in the previous step using the Lync Certificate Wizard. This certificate is used to authorize the requests coming from the IIS server.
9. After the certificate is created, view the certificate. On the Details tab click **Copy to File**. This launches the Certificate Export Wizard. Export the certificate with the private key to a file. This creates a .pfx (Personal Information Exchange) file with the certificate name.

16.2.3.2.5 Adding AllowedDomains Using WBemTest

1. To start `WBemTest.exe`, type `WBemTest` in a command prompt and click the Enter button.

2. In the Windows Management Instrumentation Tester dialog box, click **Connect**.
3. In the Connect dialog box, click **Connect**.
4. In the Windows Management Instrumentation Tester dialog box, click **Enum Classes**.
5. In the Superclass Info dialog box, click **OK**.
6. In the Query Result dialog box, scroll down to **MSFT_SIPDomainData()**, and double-click this entry.
7. In the Object editor for MSFT_SIPDomainData dialog box, click **Instances**. This causes the Query Result dialog box to open, displaying the InstanceIDs for any instances of the MSFT_SIPDomainData WMI class. These entries are the AllowedDomain entries.
8. To add AllowedDomain entries, click **Add**.
9. In the Instance of MSFT_SIPDomainData dialog box, in the Properties listbox, double-click **Address**.
10. In the Property Editor dialog box, select the **Not NULL** radio button.
11. In the Value text input pane, enter the Lync server domain; for example, `contoso.com`. Click **Save Property**.
12. In the Instance of MSFT_SIPDomainData dialog box, in the Properties listbox, double-click **Authoritative**. The Authoritative property should not be Null and should be set to False. Click **Save Property**.
13. In the Instance of MSFT_SIPDomainData dialog box, in the Properties listbox, double-click **Default Domain**. The Default Domain property should not be Null and should be set to True. Click **Save Property**.
14. In the Instance of MSFT_SIPDomainData dialog box, click **Save Object**.

16.2.3.2.6 Migrating Trusted Service Entries Using Topology Builder or PowerShell Cmdlets

To migrate trusted service entries using Microsoft Lync Server 2010 Topology Builder:

1. Launch Microsoft Lync Server 2010, Topology Builder.
2. After the existing topology is loaded, under Action, select Merge 2007 or 2007 R2 Topology. This launches a wizard.
3. Go through the wizard, keeping the default options. After the wizard has finished, check that it completed successfully. There should be no errors in the user interface.
4. Select Publish Topology and complete the wizard, as in the previous step.

To migrate trusted service entries using Microsoft Lync Server 2010 PowerShell Cmdlets:

1. From the Start menu, in the Microsoft Lync Server 2010 program group, open Lync Server Management Shell.
2. Run the following PowerShell cmdlet:

```
Merge-CsLegacyTopology -TopologyXmlFileName D:\output.xml
```
3. Run the following PowerShell cmdlet:

```
Publish-CsTopology -FileName D:\output.xml
```

16.2.3.2.7 IIS Server Configuration Because the IIS server hosts WebCenter Portal's Proxy application in the remote deployment scenario, use the information from the previous section to make it a trusted authority.

1. Install the certificate issued by the Lync server with the private key: Copy the .pfx file generated in step 7 under section "[Provisioning WebCenter Portal's Proxy Application on Lync Server](#)" to the IIS box, and double-click it. This launches the Certificate Import wizard. Import the certificate in Personal Folder under LOCAL_MACHINE.

2. Make an entry in C:/WINDOWS/system32/drivers/etc/hosts for the pool name of the Lync server as follows:

```
<ip-address-of-lync-box> <poolname-of-lync-box>
```

For example:

```
10.177.252.146 pool01.example.com
```

3. Because the IIS server hosts WebCenter Portal's Proxy application, install Microsoft UCMA v2.0 on it.

For detailed information, see [Section 16.2.3.2.8, "Installing UCMA v2.0."](#)

4. After UCMA is installed, deploy this proxy application on the IIS server. WebCenter Portal's Proxy application provides web services for interacting with Lync and sending/receiving information. WebCenter Portal talks to these web services and presents the data.

For detailed information, see [Section 16.2.3.2.9, "Installing WebCenter Portal's Proxy Application."](#)

5. Go to the location where WebCenter Portal's Proxy application was extracted. Open Web.config and edit the appSettings XML node to add the values noted in Step 7 in previous section. Ensure to set value for RemoteDeployment to true.

For example, the appSettings XML node should look somewhat like this.

```
<appSettings>
  <add key="ApplicationName" value="WebCenterProxyApplication"/>
  <add key="RemoteDeployment" value="true"/>
  <add key="ApplicationFQDN" value="iis.server.com"/>
  <add key="ApplicationGRUU"
value="sip:iis.server.com@EXAMPLE.COM;gruu;opaque=srvr:WebCenterProxyApplicatio
n:7mhSo94PlUK-5Q2bKPLyMAAA"/>
  <add key="ApplicationPort" value="6001"/>
</appSettings>
```

Note: If you see the following exception in the log file:

```

ErrorCode = -2146893039
FailureReason = NoAuthenticatingAuthority
e.Message = "Unable to perform authentication of credentials."
base {Microsoft.Rtc.Signaling.FailureResponseException} = {"Unable
to perform authentication of credentials."}
InnerException = {"NegotiateSecurityAssociation failed, error:
\_-2146893039"}

```

then add the following entry to `Web.config`:

```

<identity impersonate="true" userName="Administrator"
password="Welcome0*" />

```

where `username` is the administrator's user name, and `password` is the administrator's password.

The trust is established, and WebCenter Portal's Proxy application can talk to the Lync server.

16.2.3.2.8 Installing UCMA v2.0 Microsoft Unified Communications Managed API v2.0 (UCMA) is an endpoint API that allows advanced developers to build server applications that can interact with the Lync environment.

In a simple deployment, the UCMA is installed on the same box as Lync. In a remote deployment, the Lync core libraries are installed on the Lync box, and the UCMA is installed on the IIS (proxy) box.

1. Download UCMA v2.0 for OCS 2010 R2 installation from the following location:
<http://www.microsoft.com/downloads/details.aspx?FamilyID=b20967b1-6cf5-4a4b-b7ae-622653ac929f&displaylang=en>

Download and run the `UcmaSDKWebDownload.msi` file. This extracts set up files to the folder `C:\Microsoft Unified Communications Managed API 2.0 SDK Installer package\amd64`.

2. Go to the directory (where the files from the previous step were extracted) and run `vcredist_x86.exe`. This installs run-time components of Visual C++ Libraries required for UCMA APIs. Go to directory called `Setup` and run `UcmaRedist.msi`. This installs the UCMA 2.0 assemblies in the GAC.

16.2.3.2.9 Installing WebCenter Portal's Proxy Application

1. Extract `owc_ocs2007.zip` from the companion CD. This creates a directory named `OCSWebServices`.
2. Open the Internet Information Services (IIS) Manager.
3. Expand the server node and then **Sites** in the IIS Manager.
4. Right-click **Default Web Site**, and then select **Add Application**. The Add Application wizard displays.
5. Enter an alias for the virtual directory in the **Alias** field, for example `RTC`.
6. Enter the path to the directory extracted from the `owc_ocs2007.zip` file. For example, if you extracted the zip file in `C:\`, then enter `C:\OCSWebServices`. Alternatively, use the **Browse** button to navigate to that directory. Click **OK**.

7. Right-click the newly created application and choose **Edit Permissions** to open the Properties dialog.
8. In the Security tab, edit permissions to grant user Everyone read permission.
9. Test the Web service by accessing the Web site from the following URL format:
`http://localhost/default_website/OCSWebService.asmx`
 where *default_website* is the virtual directory you created for the Oracle RTC Web service.
 For example:
`http://localhost/RTC/OCSWebService.asmx`

16.2.3.3 Microsoft Lync - Security Considerations

You must configure an external application for Microsoft Lync connections so that users can supply credentials to authenticate themselves on the Lync server.

With a secured application, users get presence status. With Lync, if security is required, then Lync should be on a private trusted network.

Lync 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.

For more information, see [Section 16.3.1, "Registering Instant Messaging and Presence Servers Using Fusion Middleware Control."](#)

16.3 Registering Instant Messaging and Presence Servers

You can register multiple presence server connections with a WebCenter Portal 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 Portal application is deployed.

This section includes the following subsections:

- [Section 16.3.1, "Registering Instant Messaging and Presence Servers Using Fusion Middleware Control"](#)
- [Section 16.3.2, "Registering Instant Messaging and Presence Servers Using WLST"](#)

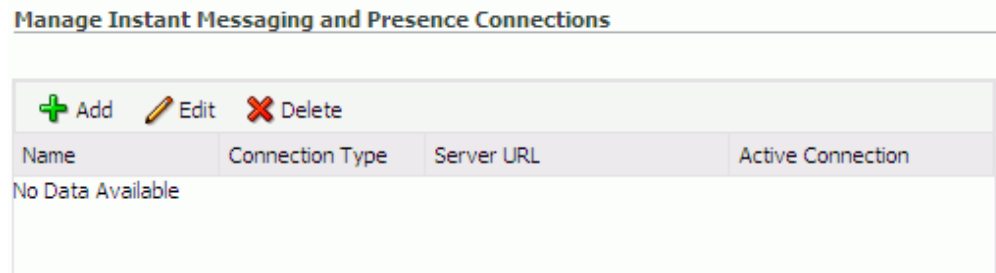
16.3.1 Registering Instant Messaging and Presence Servers Using Fusion Middleware Control

To register a presence server connection:

1. Log in to Fusion Middleware Control and navigate to the home page for the WebCenter Portal application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.

3. From the list of services on the WebCenter Portal Service Configuration page, choose **Instant Messaging and Presence**.
4. To connect to a new presence server, click **Add** (Figure 16–7).

Figure 16–7 *Configuring Instant Messaging and Presence Services*



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 (Table 16–1).

Table 16–1 *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 Portal application.
Connection Type	Specify the type of presence server: <ul style="list-style-type: none"> ■ Microsoft Live Communications Server (LCS) ■ Microsoft Office Communications Server 2007 (OCS) Out-of-the-box, WebCenter Portal supports Microsoft LCS, OCS, and Lync. Note: Microsoft Lync connections use the Microsoft Office Communications Server 2010 connection type. (Oracle Beehive Server connections are not supported in this release.)
Active Connection	Select to use this connection in the WebCenter Portal application for instant messaging and presence services. While you can register multiple presence server connections for an application, only one connection is used by the IMP service—the default (or active) connection.

6. Enter connection details for the server hosting instant messaging and presence services (Table 16–2).

Table 16–2 *Instant Messaging and Presence Connection - Connection Details*

Field	Description
Server URL	Enter the URL of the server hosting instant messaging and presence services. For example: <code>http://myocshost.com:8888</code>

Table 16–2 (Cont.) Instant Messaging and Presence Connection - Connection Details

Field	Description
User Domain	<p>(OCS/Lync Only) Enter the name of the Active Directory domain (on the Microsoft Office Communications Server) that is associated with this connection. The user domain is mandatory for OCS/Lync connections.</p> <p>Refer to Microsoft documentation for details on the user domain.</p>
Pool Name	<p>Enter the name of the pool that is associated with this connection. The pool name is mandatory.</p> <p>Refer to Microsoft documentation for details on the pool name.</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.</p> <p>You can select an existing external application from the list, or click Create New 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). For more information, see Chapter 26, "Managing External Applications."</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 Portal 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>

- Sometimes, additional parameters are required to connect to the presence server. If additional parameters are required to connect to the presence server, expand **Additional Properties** and enter details as required ([Table 16–3](#)).

Table 16–3 Instant Messaging and Presence Connection - Additional Properties

Field	Description
Add	<p>Click Add to specify an additional connection parameter:</p> <ul style="list-style-type: none"> ■ Name -Enter the name of the connection property. ■ Value - Enter the default value for the property. ■ Is Property Secured - Indicate whether encryption is required. When selected, the property value is stored securely using encryption. <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 Delete to remove a selected property.</p> <p>Select the correct row before clicking Delete.</p> <p>Note: Deleted rows appear disabled until you click OK.</p>

- Click **OK** to save this connection.

9. To start using the new (active) connection you must restart the managed server on which the WebCenter Portal application is deployed. For more information, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

16.3.2 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 the section, "createIMPConnection" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.13.3.1, "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`. For more information, see [Section 16.4.2, "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 Portal application is deployed. For more information, see the section, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in *Oracle Fusion Middleware Administrator's Guide*.

16.4 Choosing the Active Connection for Instant Messaging and Presence

You can register multiple instant messaging and presence server connections with a WebCenter Portal application, but only one connection is active at a time. The *active connection* becomes the back-end presence server for the application.

This section includes the following subsections:

- [Section 16.4.1, "Choosing the Active Connection for Instant Messaging and Presence Using Fusion Middleware Control"](#)
- [Section 16.4.2, "Choosing the Active Connection for Instant Messaging and Presence Using WLST"](#)

16.4.1 Choosing the Active Connection for Instant Messaging and Presence Using Fusion Middleware Control

To change the active connection:

1. Log in to Fusion Middleware Control and navigate to the home page for the WebCenter Portal application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.

3. From the list of services on the WebCenter Portal Services Configuration page, select **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** checkbox.
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 Portal application is deployed. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

16.4.2 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 the section, "setIMPConnection" in *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. For more information, see the section, "removeIMPServiceProperty" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

Note: To start using this active connection you must restart the managed server on which the WebCenter Portal application is deployed. For more information, see the section, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in *Oracle Fusion Middleware Administrator's Guide*.

16.5 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 Portal application is deployed.

This section includes the following subsections:

- [Section 16.5.1, "Modifying Instant Messaging and Presence Connections Details Using Fusion Middleware Control"](#)
- [Section 16.5.2, "Modifying Instant Messaging and Presence Connections Details Using WLST"](#)

16.5.1 Modifying Instant Messaging and Presence Connections Details Using Fusion Middleware Control

To update connection details for an instant messaging and presence server:

1. Log in to Fusion Middleware Control and navigate to the home page for the WebCenter Portal application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
3. From the list of services on the WebCenter Portal Service Configuration page, select **Instant Messaging and Presence**.
4. Select the connection name, and click **Edit**.
5. Edit connection details, as required. For detailed parameter information, see [Table 16–2, "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 Portal application is deployed. For more information, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

16.5.2 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 the section, "setIMPConnection" in *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 more information, see the section, "setIMPConnectionProperty" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.13.3.1, "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 Portal application is deployed. For more information, see the section, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in *Oracle Fusion Middleware Administrator's Guide*.

16.6 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. When you delete the active connection, user presence options are not 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. For more information, see [Section 26.5, "Deleting External Application Connections."](#)

This section includes the following subsections:

- [Section 16.6.1, "Deleting Instant Messaging and Presence Connections Using Fusion Middleware Control"](#)
- [Section 16.6.2, "Deleting Instant Messaging and Presence Connections Using WLST"](#)

16.6.1 Deleting Instant Messaging and Presence Connections Using Fusion Middleware Control

To delete an instant messaging and presence server connection:

1. Log in to Fusion Middleware Control and navigate to the home page for the WebCenter Portal application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
3. From the list of services on the WebCenter Portal Service Configuration page, select **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 Portal application is deployed. For more information, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

Note: Before restarting the managed server, mark another connection as active; otherwise, the service is disabled.

16.6.2 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 the section, "deleteConnection" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

16.7 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`: Determines what to display if user display names are missing. When set to 0, and display name information is unavailable, only the user name displays in the application. When set to 1, and display name information is unavailable, display names are read from user profile data. Setting this option to 1 impacts performance. The default setting is 0.

Display names are not mandatory in presence data. If the WebCenter Portal application does not always provide display names by default and you consider this information important, set `resolve.display.name.from.user.profile` to 1 so that display names always display.

- `im.address.resolver.class`: Resolver implementation used to map user names to IM addresses and IM addresses to user names. The default setting is `oracle.webcenter.collab.rtc.IMPAddressResolverImpl`. This implementation looks for IM addresses in the following places and order:
 - User Preferences
 - User Credentials
 - User Profiles
- `im.address.profile.attribute`: User profile attribute used to determine a user's IM address. The default setting is `BUSINESS_EMAIL`. Users can change this default with `im.address.profile.attribute`.

For command syntax and detailed examples, see the section, "setIMPServiceProperty" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

16.8 Testing Instant Messaging and Presence Connections

Web services expose a set of Web methods that you can invoke to test the validity. To verify a connection, try accessing the endpoint for the WebCenter Portal RTC Web services deployed on it. For example (assuming the application context path is `/RTC`):

- `protocol://host/RTC/ApplicationConfigurationService.asmx`
- `protocol://host/RTC/RTCService.asmx`
- `protocol://host/RTC/OCSWebService.asmx`

Managing the Mail Service

This chapter describes how to configure and manage the Mail service for Oracle WebCenter Portal applications. It also describes how to configure the "Send Mail" feature, which allows application resources to send mail directly from them. The Send Mail feature does not require the Mail service. That is, even if the Mail service has not been configured in your application, users can send mail notifications with the local mail client. For more information on using the Send Mail notifications, see the section "What You Should Know About the Send Mail Feature" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

Always use Fusion Middleware Control or WLST command-line tool to review and configure back-end services for WebCenter Portal applications. Any changes that you make to WebCenter Portal applications, post deployment, are stored in MDS metadata store as customizations. See [Section 1.3.5, "WebCenter Portal Configuration Considerations."](#)

Note: Configuration changes for the Mail service, through Fusion Middleware Control or using WLST, are not dynamic so you must restart the managed server on which the WebCenter Portal application is deployed for your changes to take effect. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

This chapter includes the following sections:

- [Section 17.1, "What You Should Know About Mail Server Connections"](#)
- [Section 17.2, "Configuration Roadmaps for the Mail Service"](#)
- [Section 17.3, "Mail Server Prerequisites"](#)
- [Section 17.4, "Registering Mail Servers"](#)
- [Section 17.5, "Choosing the Active \(or Default\) Mail Server Connection"](#)
- [Section 17.6, "Modifying Mail Server Connection Details"](#)
- [Section 17.7, "Deleting Mail Server Connections"](#)
- [Section 17.8, "Setting Up Mail Service Defaults"](#)
- [Section 17.9, "Testing Mail Server Connections"](#)
- [Section 17.10, "Troubleshooting Issues with Mail"](#)

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."](#)

17.1 What You Should Know About Mail Server Connections

WebCenter Portal supports the Microsoft Exchange Server or any mail server that supports IMAP4 and SMTP. To enable users to access mail within a WebCenter Portal application and perform basic operations such as read, reply, and forward, you must first register the appropriate mail server with the WebCenter Portal application. The Mail service is not configured out-of-the-box.

You can register multiple mail server connections:

- **WebCenter Portal: Spaces** applications support multiple mail connections. The mail connection marked *active* is the default connection for mail services in Spaces. All additional connections are offered as alternatives; Spaces users can choose which one they want to use through user preferences.
- **WebCenter Portal: Framework** application only use one mail connection—the connection marked *active*. Any additional connections are ignored.

17.2 Configuration Roadmaps for the Mail Service

Use the roadmaps in this section as an administrator's guide through the configuration process:

- **Roadmap - Configuring the Mail Service for Framework Applications**

[Figure 17-1](#) and [Table 17-1](#) provide an overview of the prerequisites and tasks required to get the Mail service working in Framework applications.

Figure 17–1 Configuring the Mail Service for Framework Applications

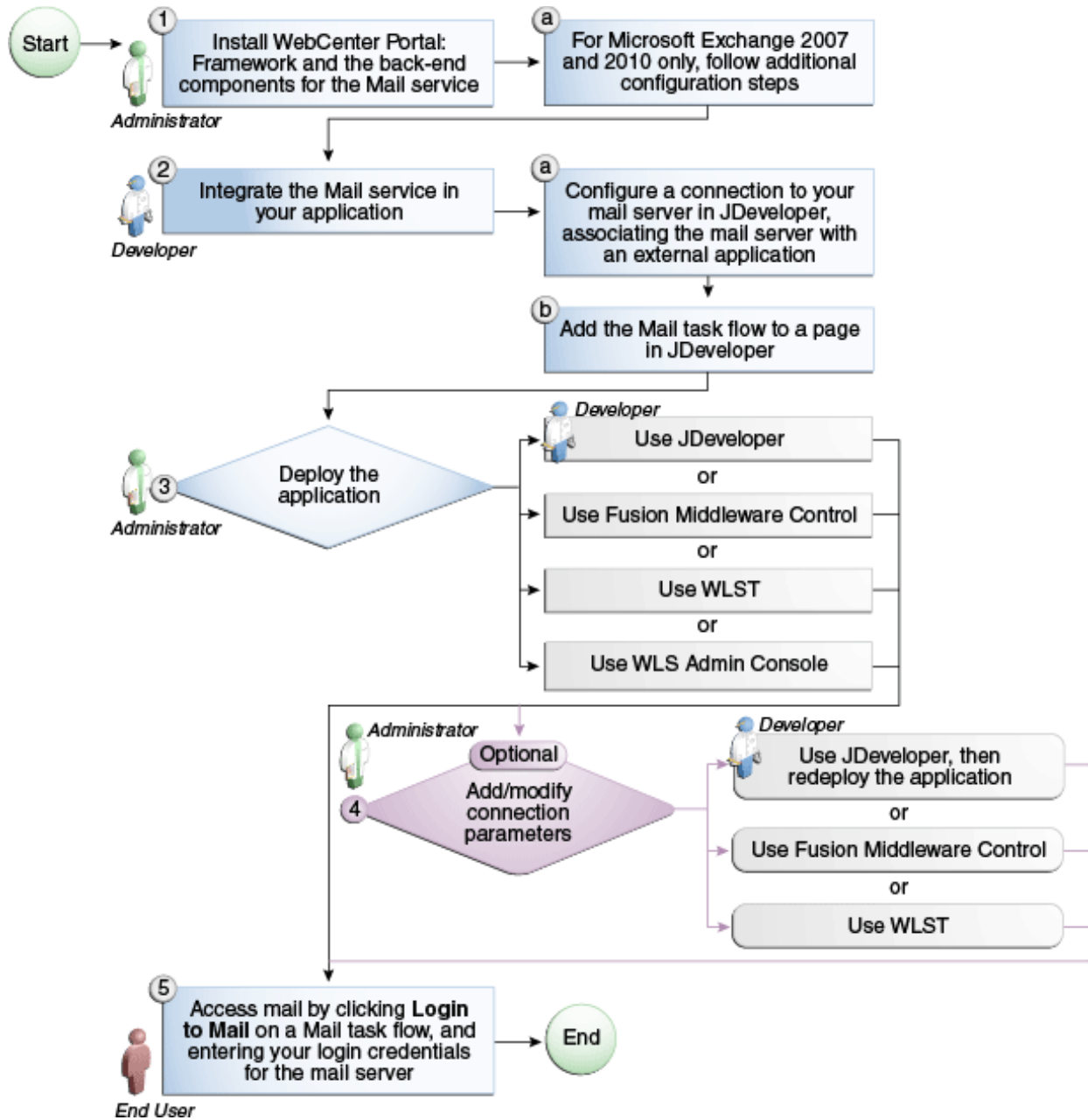


Table 17–1 Configuring the Mail Service for Framework Applications

Actor	Task	Sub-task
Administrator	1. Install WebCenter Portal and the back-end components for the Mail service	1.a For Microsoft Exchange 2007 and 2010 only, follow additional configuration steps
Developer	2. Integrate the Mail service in your Framework application	2.a Configure a connection to your mail server in JDeveloper, associating the mail server with an external application 2.b Add the Mail task flow to a page in JDeveloper

Table 17–1 (Cont.) Configuring the Mail Service for Framework Applications

Actor	Task	Sub-task
Developer or Administrator	3. Deploy the Framework application using one of the following tools:	<ul style="list-style-type: none"> ▪ JDeveloper (Developer) ▪ Fusion Middleware Control (Administrator) ▪ WLST (Administrator) ▪ WLS Admin Console (Administrator)
Developer or Administrator	4. (Optional) Add/modify connection parameters using one of the following tools:	<ul style="list-style-type: none"> ▪ JDeveloper, then redeploy the application (Developer) ▪ Fusion Middleware Control (Administrator) ▪ WLST (Administrator)
End User	5. Access mail by clicking Login to Mail on a Mail task flow, and entering your login credentials for the mail server	

▪ **Roadmap - Configuring the Mail Service for Spaces Applications**

Figure 17–2 and Table 17–2 provide an overview of the prerequisites and tasks required to get the Mail service working in Spaces.

Figure 17-2 Configuring the Mail Service for Spaces Applications

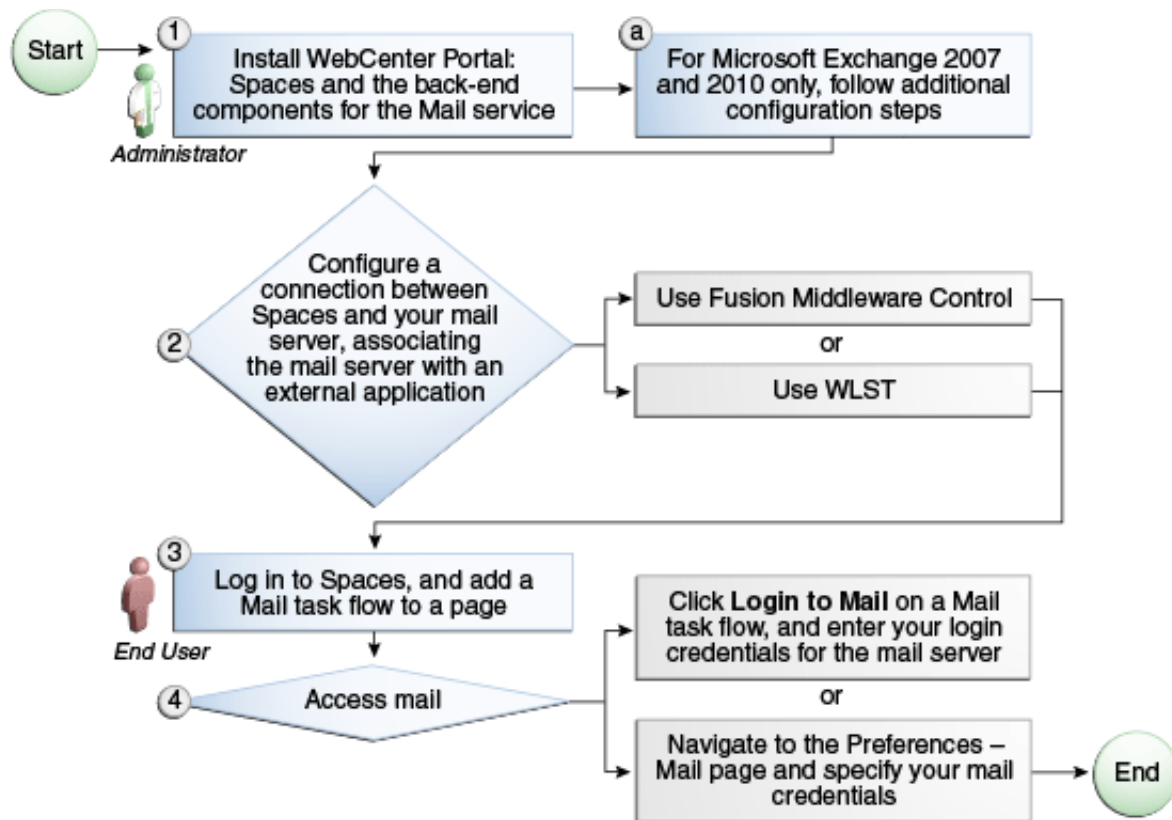


Table 17-2 Configuring the Mail Service for Spaces Applications

Actor	Task	Sub-task
Administrator	1. Install WebCenter Portal and the back-end components for the Mail service	1.a For Microsoft Exchange 2007 and 2010 only, follow additional configuration steps
	2. Configure a connection between Spaces and your mail server -- associating the mail server with an external application -- using one of the following tools: <ul style="list-style-type: none"> ■ Fusion Middleware Control ■ WLST 	
End User	3. Add the Mail task flow to the Spaces page	
	4. Access mail with one of the following methods: <ul style="list-style-type: none"> ■ Click Login to Mail on a Mail task flow, and entering your login credentials for the mail server ■ Navigate to the Preferences - Mail page and specify your mail credentials 	

17.3 Mail Server Prerequisites

This section includes the following subsections:

- [Section 17.3.1, "Mail Server - Installation"](#)

- [Section 17.3.2, "Mail Server - Configuration"](#)
- [Section 17.3.3, "Mail Server - Security Considerations"](#)
- [Section 17.3.4, "Mail Server - Limitations"](#)

17.3.1 Mail Server - Installation

See your mail server documentation for installation information.

17.3.2 Mail Server - Configuration

You can allow WebCenter Portal to create and manage space distribution lists in Spaces (or in Framework applications leveraging WebCenter Portal: Spaces space management). This feature is supported only with Microsoft Exchange.

The space distribution list is created automatically whenever a space is created. Users added or removed from the space are implicitly added or removed from the corresponding space distribution list, provided that the LDAP Base DN does not change (only one LDAP Base DN is supported) and that users created on Microsoft Exchange Active Directory correspond with users created in the identity store used by the WebCenter Portal application. To disable this feature, do not enter the LDAP (Active Directory) server details in the mail connection.

For more information, see step 7 of [Section 17.4.1, "Registering Mail Servers Using Fusion Middleware Control."](#)

For information about adding users on a mail server, see the mail server's product documentation. For information about adding users to the WebCenter Portal application's identity store, see [Section 29.4, "Adding Users to the Embedded LDAP Identity Store."](#)

Microsoft Exchange 2007 and Microsoft Exchange 2010 are the only mail servers for which there are configuration prerequisites. If you are working with a different mail server (including Microsoft Exchange 2003), then you can skip the rest of this section.

17.3.2.1 Configuring Microsoft Exchange Server 2007 or 2010 for WebCenter Portal

The Microsoft Exchange Server 2007 or Exchange Server 2010 certificate must be added to the WebCenter Portal keystore. This requires the following steps.

1. [Section 17.3.2.1.1, "Obtain the Certificate from the Microsoft Exchange Server"](#)
2. [Section 17.3.2.1.2, "Add the Certificate to the WebCenter Portal Keystore"](#)
3. Restart the server after the certificate is imported.

17.3.2.1.1 Obtain the Certificate from the Microsoft Exchange Server Obtain the certificate from your mail server installation administrator. This section describes one way to get the certificate from the Microsoft Exchange Server.

Follow these steps to obtain the certificate from a Microsoft Exchange 2007 or 2010 server.

1. Open a browser and connect to your IMAP server with the following command:

```
https://host_name/owa
```

Where *host_name* is the name of the Microsoft Exchange Server.

2. Place your cursor on the page, right-click, and select **Properties**, then click **Certificate**.

3. 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.
4. Convert the .DER format certificate to .PEM format.

Note: WebLogic only recognizes .PEM format.

Use Firefox 3.0 or later to download the certificate directly to .PEM format. For other browsers, use the WebLogic Server `der2pem` tool to convert to .PEM format. For more information about `der2pem` see *Oracle Fusion Middleware Command Reference for Oracle WebLogic Server*.

17.3.2.1.2 Add the Certificate to the WebCenter Portal Keystore

1. Import the downloaded certificate into the keystore, which is generally the file named `cacerts` in the `JAVA_HOME`. For example:

```
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. In a standard installation, the `JAVA_HOME` is in the following location:

```
/scratch/wcinstall/ps2/1225/wlshome/jrockit_160_17_R28.0.0-616
```

See [Section 31.4.2.1.3, "Configuring and Exporting the Certificates,"](#) for information about adding the certificate to the keystore.

2. Restart the server.

17.3.2.1.3 Microsoft Exchange Server Considerations

- The IMAP port is 993 and secured true. SMTP port is 587 and secured true. (Microsoft Exchange Server 2005 used 465.)
- If you see the following error, then you must change the trust store entry in the domain startup file `setDomainEnv.sh`:

```
Caused by: java.io.IOException: Keystore was tampered with, or password was
incorrect
    at sun.security.provider.JavaKeyStore.engineLoad(JavaKeyStore.java:771)
    at sun.security.provider.JavaKeyStore$JKS.engineLoad(JavaKeyStore.java:38)
    at java.security.KeyStore.load(KeyStore.java:1185)
    at com.sun.net.ssl.internal.ssl.TrustManagerFactoryImpl.getCacertsKeyStore
(TrustManagerFactoryImpl.java:202)
    at com.sun.net.ssl.internal.ssl.DefaultSSLContextImpl.getDefaultTrustManager
(DefaultSSLContextImpl.java:70)
```

To change the entry:

- a. Shutdown the managed server on which WebCenter Portal is deployed.
- b. Edit the domain startup script `setDomainEnv` located at:

```
UNIX: DOMAIN_HOME/bin/setDomainEnv.sh
```

```
Windows: DOMAIN_HOME\bin\setDomainEnv.cmd
```

- c. Add the Java property, as follows:

```
-Djavax.net.ssl.trustStore=<path to truststore>
```

```
-Djavax.net.ssl.trustStorePassword=<truststore password>
```

For example:

```
set JAVA_PROPERTIES=  
-Dplatform.home=%WL_HOME% -Dwls.home=%WLS_HOME% -Dweblogic.home=%WLS_HOME%  
-Djavax.net.ssl.trustStore=C:\jive\mailtool\jssecacerts  
-Djavax.net.ssl.trustStorePassword=changeit
```

- d. Restart the managed server.

17.3.3 Mail Server - Security Considerations

For more information, see [Section 33.8, "Securing the 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. For more information, see [Table 17-5](#).

17.3.4 Mail Server - Limitations

In WebCenter Portal: Spaces, the Mail service requires a Microsoft Exchange mail server connection to enable automatic space distribution list management.

17.4 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 Portal application is deployed.

This section includes the following subsections:

- [Section 17.4.1, "Registering Mail Servers Using Fusion Middleware Control"](#)
- [Section 17.4.2, "Registering Mail Servers Using WLST"](#)




17.4.1 Registering Mail Servers Using Fusion Middleware Control

To register a mail server with WebCenter Portal applications:

1. Log in to Fusion Middleware Control and navigate to the home page for the WebCenter Portal application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
3. From the list of services on the WebCenter Portal Service Configuration page, select **Mail Server**.
4. To connect to a new mail server, click **Add** ([Figure 17-3](#)).

Figure 17-3 Configuring Mail Servers

Manage Mail Server Connections

 Add
  Edit
  Delete

Name	IMAP Host	SMTP Host	Active Connection
------	-----------	-----------	-------------------

5. Enter a unique name for this connection, and indicate whether this connection is the active (or default) connection for the application (Table 17-3).

Table 17-3 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 Portal 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"> ▪ WebCenter Portal: Spaces applications support multiple mail connections. The mail connection marked <i>active</i> is the default connection for mail services in Spaces. All additional connections are offered as alternatives; Spaces users can choose which one they want to use through user preferences. ▪ WebCenter Portal: Framework applications only use one mail connection—the connection marked <i>active</i>. Any additional connections are ignored.

6. Enter connection details for the mail server (Table 17-4).

Table 17-4 Mail Server Connection Parameters

Field	Description
IMAP Host	Enter the host name of the computer 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.
SMTP Host	Enter the host name of the computer 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.

Table 17–4 (Cont.) Mail Server Connection Parameters

Field	Description
Associated External Application	<p>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 uses the same credentials to authenticate the user on both IMAP and SMTP.</p> <p>You can select an existing external application from the list, or click Create New to configure a new external application. For more information, see Chapter 26, "Managing External Applications."</p> <p>The external application for the Mail service must use <code>Authentication Method=POST</code>, and you can customize some mail header fields (with Display to User enabled):</p> <ul style="list-style-type: none"> Property: <code>mail.user.emailAddress</code> (who the mail is from) Property: <code>mail.user.displayName</code> (display name from the mail) Property: <code>mail.user.replyToAddress</code> (address used to reply to the mail) <p>These properties ensure that a specific mail address is the same in the external application and in the mail server. They are added to the Mail connection and are used by the Mail service for the From, Display Name and Reply To fields (Figure 17–4).</p> <p>If your WebCenter Portal application offers a self-registration page with the facility to mail user ID information on request, then you must ensure that public credentials are configured for the external application selected here. If public credentials are not defined, then mails cannot be sent to users on their request. The Spaces application, for example, offers this feature on its default self-registration page.</p>

Figure 17–4 Additional Properties for Mail Connection

Additional Properties

Enter names and values for any additional properties.

+ Add ✗ Delete		
Property Name	Property Value	Is Property Secured?
mail.user.emailAddress	john.doe@example.com	<input type="checkbox"/>
mail.user.displayName	John Doe	<input type="checkbox"/>
mail.user.replyToAddress	feedback@example.com	<input type="checkbox"/>

- Specify LDAP connection details for the Active Directory server managing space distribution lists ([Table 17–5](#)).

This section applies to Spaces (or Framework applications leveraging the space management feature). WebCenter Portal 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 *distribution lists* to work in Spaces.

Table 17–5 LDAP Directory Server Configuration Parameters

Field	Description
LDAP Host	Enter the host name of the computer 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	Enter the domain appended to distribution list names. In Spaces, for example, if the domain value is set to <code>example.com</code> , then a space named Finance Project maintains a distribution list named <code>FinanceProject@example.com</code> .
LDAP Admin User	Enter the user name of the LDAP directory server administrator. A valid user with privileges to make entries into the LDAP schema.
LDAP Admin Password	Enter the password for the LDAP directory server administrator. The password is stored in a secured store.
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 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 Portal application and the LDAP directory server.

8. Configure advanced options for the mail server connection ([Table 17–6](#)).

Table 17–6 Mail Server Connection - Advanced Configuration

Field	Description
Connection Timeout (in Seconds)	Specify a suitable timeout for the connection. This is the length of time (in seconds) the WebCenter Portal application waits for a response from the mail server before issuing a connection timeout message. The default is -1, which means that the service default is used. The service default is 10 seconds.

9. Optionally, you can add more parameters to the mail server connection ([Table 17–7](#)).

Table 17–7 Additional Mail Connection Properties

Additional Connection Property	Description
<code>charset</code>	Character set used on the connection. The default charset is UTF-8. To use a different character set, such as ISO-8859-1, set the charset connection property.

Table 17–7 (Cont.) Additional Mail Connection Properties

Additional Connection Property	Description
Various IMAP properties	<p>Any valid IMAP connection property. For example, <code>mail.imap.connectionpoolsize</code>.</p> <p>For a list of valid protocol properties, see your mail server documentation. For a list of standard IMAP properties, see the Java Mail APIs:</p> <p>http://java.sun.com/products/javamail/javadocs/com/sun/mail/imap/package-summary.html</p>
Various SMTP properties	<p>Any valid SMTP connection property. For example, <code>mail.smtp.timeout</code>.</p> <p>For a list of valid protocol properties, see your mail server documentation. For a list of standard SMTP properties, see the Java Mail APIs:</p> <p>http://java.sun.com/products/javamail/javadocs/com/sun/mail/smtp/package-summary.html</p>

If additional parameters are required to connect to the mail server, expand **Additional Properties** and enter details as required (see [Table 17–8, "Mail Connection - Additional Properties"](#)).

Table 17–8 Mail Connection - Additional Properties

Field	Description
Add	<p>Click Add to specify an additional connection parameter:</p> <ul style="list-style-type: none"> ▪ Name -Enter the name of the connection property. ▪ Value - Enter the default value for the property. ▪ Is Property Secured - Indicate whether encryption is required. When selected, the property value is stored securely using encryption. <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 Delete to remove a selected property.</p> <p>Select the correct row before clicking Delete.</p> <p>Note: Deleted rows appear disabled until you click OK.</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 Portal application is deployed. For more information, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

17.4.2 Registering Mail Servers Using WLST

Use the WLST command `createMailConnection` to create a mail server connection. For command syntax and examples, see the section, "createMailConnection" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

Use the WLST command `setMailConnectionProperty` to add additional required properties through your external application. The external application for the Mail

service must use Authentication Method=POST, and you can customize some mail header fields (with Display to User enabled). For example:

```
setMailConnectionProperty(appName='webcenter', name='NotificationSharedConn',
key='mail.user.emailAddress', value='john.doe@example.com')
```

```
setMailConnectionProperty(appName='webcenter', name='NotificationSharedConn',
key='mail.user.displayName', value='John Doe')
```

```
setMailConnectionProperty(appName='webcenter', name='NotificationSharedConn',
key='mail.user.replyToAddress', value='feedback@example.com')
```

where:

- `mail.user.emailAddress` = Email Address ('From' from the mail)
- `mail.user.displayName` = Your Name (display name from the mail)
- `mail.user.replyToAddress` = Reply-To Address (address when replying to the mail)

These properties ensure that a specific mail address is the same in the external application and in the mail server. These properties are added to the Mail connection and are used by the Mail service for the From, Display Name and Reply To fields.

If your WebCenter Portal application offers a self-registration page with the facility to mail user ID information on request, then you must ensure that public credentials are configured for the external application selected here. If public credentials are not defined, then mails cannot be sent to users on their request. The Spaces application, for example, offers this feature on its default self-registration page.

For command syntax and examples, see the section, "setMailConnectionProperty" in *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`. For more information, see [Section 17.5.2, "Choosing the Active \(or Default\) Mail Server Connection Using WLST."](#)

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

Note: To start using new connections you must restart the managed server on which the WebCenter Portal application is deployed. For more information, see the section, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in *Oracle Fusion Middleware Administrator's Guide*.

17.5 Choosing the Active (or Default) Mail Server Connection

You can register multiple mail server connections with a WebCenter Portal application but only one connection can be designated as the default connection. The *default connection* becomes the back-end mail server for:

- Mail task flows
- Space distribution lists
- Anywhere there is a **Send Mail** icon

This section includes the following subsections:

- [Section 17.5.1, "Choosing the Active \(or Default\) Mail Server Connection Using Fusion Middleware Control"](#)
- [Section 17.5.2, "Choosing the Active \(or Default\) Mail Server Connection Using WLST"](#)

17.5.1 Choosing the Active (or Default) Mail Server Connection Using Fusion Middleware Control

To change the default connection:

1. Log in to Fusion Middleware Control and navigate to the home page for the WebCenter Portal application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
3. From the list of services on the WebCenter Portal Services Configuration page, select **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** checkbox.
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 Portal application is deployed. For more information, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

17.5.2 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 the section, "setMailConnection" in *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. For more information, see the section, "removeMailServiceProperty" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

Note: To start using the active connection you must restart the managed server on which the WebCenter Portal application is deployed. For more information, see the section, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in *Oracle Fusion Middleware Administrator's Guide*.

17.6 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 Portal application is deployed.

This section includes the following subsections:

- [Section 17.6.1, "Modifying Mail Server Connection Details Using Fusion Middleware Control"](#)
- [Section 17.6.2, "Modifying Mail Server Connection Details Using WLST"](#)

17.6.1 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 the WebCenter Portal application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
3. From the list of services on the WebCenter Portal Service Configuration page, select **Mail Server**
4. Select the connection name, and click **Edit**.
5. Edit connection details, as required. For detailed parameter information, see [Table 17-4, "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 Portal application is deployed. For more information, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

17.6.2 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 the section,

"setMailConnection" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

If additional parameters are required to connect to your mail server, use the `setMailConnectionProperty` command. For more information, see the section, "setMailConnectionProperty" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

Note: To start using the updated connections you must restart the managed server on which the WebCenter Portal application is deployed. For more information, see the section, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in *Oracle Fusion Middleware Administrator's Guide*.

17.7 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 do not 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. For more information, see [Section 26.5, "Deleting External Application Connections."](#)

This section includes the following subsections:

- [Section 17.7.1, "Deleting a Mail Connection Using Fusion Middleware Control"](#)
- [Section 17.7.2, "Deleting a Mail Connection Using WLST"](#)

17.7.1 Deleting a Mail Connection Using Fusion Middleware Control

To delete a mail server connection:

1. Log in to Fusion Middleware Control and navigate to the home page for the WebCenter Portal application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
3. From the list of services on the WebCenter Portal Services Configuration page, select **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 Portal application is deployed. For more information, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

Note: Before restarting the managed server, mark another connection as active; otherwise, the service is disabled.

17.7.2 Deleting a Mail Connection Using WLST

Use the WLST command `deleteConnection` to remove a mail server connection. For command syntax and examples, see the section, "deleteConnection" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

17.8 Setting Up Mail Service Defaults

Use the WLST command `setMailServiceProperty` to set defaults for the Mail service:

- `address.delimiter`: Defines the delimiter that is used to separate multiple mail addresses. A comma is used by default.

Some mail servers require mail addresses in the form lastname, firstname and, in such cases, a semicolon is required.

- `mail.emailgateway.polling.frequency`: Frequency, in seconds, that space distribution lists are checked for new incoming mails. The default is 1800 seconds (30 minutes).

Email communication through space distribution lists can be published as discussion forum posts on a discussions server. For details, see "Publishing Space Mail in a Discussion Forum" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

- `mail.messages.fetch.size`: Maximum number of messages displayed in mail inboxes
- `resolve.email.address.to.name`: Determines whether user email addresses are resolved to WebCenter Portal user names when LDAP is configured. Valid values are 1 (true) and 0 (false). The default value is 0.

When set to 1, WebCenter Portal user names display instead of email addresses in Mail task flows.

Set this property to 1 if the Instant Messaging and Presence service requires user names to obtain presence status because presence information cannot be obtained when the Mail service provides email addresses. Setting this value to 1 does impact application performance so you must take this into consideration when setting this property.

For command syntax and examples, see the section, "setMailServiceProperty" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

17.9 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)

17.10 Troubleshooting Issues with Mail

This section includes the following subsections:

- [Section 17.10.1, "Mail Service is Not Accessible in Secure Mode"](#)
- [Section 17.10.2, "Mail Service is Not Accessible in Non-Secure Mode"](#)
- [Section 17.10.3, "Unable to Create Distribution Lists in the Non-Secure Mode"](#)
- [Section 17.10.4, "Unable to Create Distribution Lists in the Secure Mode"](#)
- [Section 17.10.5, "Unable to Configure the Number of Mails Downloaded"](#)
- [Section 17.10.6, "Unable to Publish and Archive Space Mail"](#)
- [Section 17.10.7, "Changing Passwords on Microsoft Exchange"](#)
- [Section 17.10.8, "Mail Content Sent as Attachments"](#)

17.10.1 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 17.4, "Registering Mail Servers."](#)
- Properties are set to `true` in your mail server.
 - `mail.imap.secured = true`
 - `mail.smtp.secured = true`

17.10.2 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 17.4, "Registering Mail Servers."](#)
- Properties are set to `false` in your mail server.
 - `mail.imap.secured = false`

```
- mail.smtp.secured = false
```

17.10.3 Unable to Create Distribution Lists in the Non-Secure Mode

Problem

You are unable to create space distribution lists in non-secure mode; that is, SSL is not 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 non-secure mode, in the LDAP server:

- ldapHost
- defaultUser
- ldapAdminPassword
- ldapBaseDN
- ldapPort

See [Section 17.4, "Registering Mail Servers."](#)

17.10.4 Unable to Create Distribution Lists in the Secure Mode

Problem

You are unable to create space distribution lists 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 Also: [Section 17.4, "Registering Mail Servers"](#)

17.10.5 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 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 *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

17.10.6 Unable to Publish and Archive Space Mail

Problem

You are unable to archive Space mail.

Solution

If the archiving fails, check the following:

- In WebCenter Portal: Spaces, navigate to Administration, Configuration, Services, Discussions. Check whether the required configuration is accurate. See also, "Enabling Discussion Forums to Publish Space Mail" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.
- Check whether the user account configured here is a member of the distribution list.
- For a particular space, check whether the forum configured is available in the discussions server. See "Publishing Space Mail in a Discussion Forum" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.
- Check whether the user who sends mails to the distribution list is available in the discussions server and his mail address is the same.

17.10.7 Changing Passwords on Microsoft Exchange

Problem

If multiple users log on to Microsoft Exchange with the same user name and password, and then one user changes the password, the original password remains valid until all users log off.

For example, say the current password of the user monty is welcome1. Two users, A and B, log on from different clients using either WebCenter Portal or Microsoft Exchange. Both log on as monty/welcome1, and both are able to see the mails. Now user A changes the password in Microsoft Exchange to oracle1. Because there currently are clients using the passwords oracle1 and welcome1, both are valid passwords; that is, new users can log on as monty/welcome1 and still see the mails.

Solution

After all existing users with the original password log off, the new password takes effect. Until then, users can use both passwords to log on.

17.10.8 Mail Content Sent as Attachments

Problem

When users receive mail in Framework applications, message content is shown as an attachment (named `content.html`) rather than within the message body. This can occur if the mail server is running Microsoft Exchange Server 2007 and the "*Update Rollup 3 for Microsoft Exchange Server 2007*" is not yet installed.

Solution

Download and install "*Update Rollup 3 for Microsoft Exchange Server 2007*" which fixes this issue. For more information, see

<http://support.microsoft.com/kb/930468>.

Managing the People Connections Service

This chapter describes backend configuration requirements for the People Connections service. Always use Fusion Middleware Control or WLST command-line tool to review and configure back-end services for WebCenter Portal applications. Any changes that you make to WebCenter Portal applications, post deployment, are stored in MDS metadata store as customizations.

This chapter includes the following sections:

- [Section 18.1, "What You Should Know About the People Connections Service"](#)
- [Section 18.2, "People Connections Prerequisites"](#)
- [Section 18.3, "Setting Up a Proxy Server for Activity Stream"](#)
- [Section 18.4, "Archiving the Activity Stream Schema"](#)

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."](#)

18.1 What You Should Know About the People Connections Service

The People Connections service provides social networking tools for creating, interacting with, and tracking the activities of one's connections. Its features enable users to manage their personal profiles, access the profiles of other users, provide *ad hoc* feedback, post messages, track activities, and connect with others.

It does this through a set of features that include:

- **Activity Stream** for viewing user activities generated through application or social networking actions.
- **Connections** for connecting to other application users to share information, comment on performance, exchange messages, and track activity
- **Feedback** for giving ad hoc performance feedback to other users
- **Message Board** for posting messages to other users
- **Profile** for entering personal contact information and viewing the contact information of other users
- **Publisher** for publishing status messages and posting files and links

The features of the People Connections service fall into the above five categories. Each category includes a set of task flows that expose People Connections features to end users.

For information about the People Connections service at runtime, see Part VIII, "Organizing Your Collaborative and Social Networking Environment," in the Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces.

For additional information about configuring People Connections, refer to "Configuring People Connections Defaults for WebCenter Spaces" in the Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces.

18.2 People Connections Prerequisites

To use the People Connections service, you must have the `WEBCENTER` schema installed in your database.

In a production environment, an enterprise can leverage its back-end identity store as a means of providing People Connections with a population of potential connections. In a development environment, developers can add test-users to the `jazn-data.xml` file.

For example, Profile takes the bulk of its information from the back-end identity store that provides your WebCenter Portal application with its users. Additionally, Profile may offer opportunities for altering some of this information and for providing additional data not included in the identity store.

For information about connecting to a back-end (LDAP) identity store for the production version of your application, see [Chapter 29, "Configuring the Identity Store"](#).

18.3 Setting Up a Proxy Server for Activity Stream

To enable external people connection feeds in your WebCenter Portal applications, you must set up a proxy server.

A proxy server is also required if you want to display external links in Activity Stream task flows. Both the People Connection service and the Activity Stream service share the same proxy server settings.

You can configure a proxy server by using either Fusion Middleware Control or WLST. For information, see [Section 9.7, "Setting Up a Proxy Server."](#)

18.4 Archiving the Activity Stream Schema

Application administrators can use WLST commands to archive and restore data in the Activity Stream schema. The following commands are available:

- `archiveASByDate`—Archive activity stream data that is older than a specified date.
- `archiveASByDeletedObjects`—Archive activity stream data associated with deleted objects.
- `archiveASByClosedSpaces`—Archive activity stream data associated with Spaces that are currently closed.
- `archiveASByInactiveSpaces`—Archive activity stream data associated with Spaces that have been inactive since a specified date.

- `restoreASByDate`—Restore archived activity stream data from a specified date into production tables.

For more information, see the section, "Activity Stream," in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

18.5 Configuring Cache Options for the Profile Service

To configure the Profile service JOC cache, for example, you use the WLST command `setProfileCacheTimeToLive` to set the idle time for an object to live in a cache after which if the object has not been accessed, it will be removed. Likewise, use the WLST command `setProfileCacheNumberOfObjects` to set the maximum number of objects that can live in the cache after which older objects or unused objects will be removed.

For command syntax and examples, see the section, "XWLSTX" in Oracle Fusion Middleware WebLogic Scripting Tool Command Reference.

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

Managing Subscriptions and Notifications

In the Spaces application, subscriptions and notifications provide users with a means of subscribing to the types of services and application objects in which they have a particular interest. Consequently, users receive timely notice of the changes that affect their subscribed services and objects from their selected messaging channels.

See Also: For more information, see the section, "What You Should Know About Subscriptions and Notifications," in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

Notifications administration provides a means of creating and, potentially, enforcing application-wide defaults for application-level subscriptions and specifying a connection type that identifies the server that will handle notification delivery.

This chapter steps through the process of performing these administrative tasks and provides information about how to set and get Notifications messaging configuration details using WLST commands.

Always use the Fusion Middleware Control or WLST command-line tool to review and configure back-end services for WebCenter Portal applications. Any changes you make to WebCenter Portal applications, post deployment, are stored in MDS metadata store as customizations. See [Section 1.3.5, "WebCenter Portal Configuration Considerations."](#)

Note: Most changes you make to WebCenter Portal services configuration through Fusion Middleware Control or using WLST are not dynamic. For your changes to take effect, you must restart the managed server to which the WebCenter Portal application is deployed. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

This chapter includes the following sections:

- [Section 19.1, "Setting Up Default Subscription Preferences"](#)
- [Section 19.2, "Setting Up Notifications"](#)
- [Section 19.3, "Creating and Applying Custom Notification Templates"](#)
- [Section 19.4, "Testing the Notifications Connection"](#)
- [Section 19.5, "Troubleshooting Issues with Notifications"](#)

19.1 Setting Up Default Subscription Preferences

Spaces users set their personal Subscriptions preferences through the Spaces application's Preferences dialog. Before this happens, the WebCenter Portal administrator can set default values that determine the application-level subscription options that are available to all users and whether those defaults can be changed.

This section provides an overview of Subscription defaults and steps you through the process of setting default values.

This section includes the following subsections:

- [Section 19.1.1, "What You Should Know About Subscription Defaults"](#)
- [Section 19.1.2, "Setting Subscription Defaults"](#)
- [Section 19.1.3, "Setting Subscriptions Preferences in Spaces"](#)

19.1.1 What You Should Know About Subscription Defaults

Administrator-level Subscription preferences are set in a custom XML file that you create and then use to supersede the file that is provided for this purpose out of the box (`notification-service-settings.xml`). The settings in the custom XML file are analogous to the application-level subscriptions settings available to users through Subscription Preferences in the Spaces application (for more information, see the section, "Setting Application-Level Subscriptions," in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.)

Each setting provides three attributes:

- `id`—for specifying the service ID:
 - `oracle.webcenter.peopleconnections.connections`, the Connections feature of the People Connections service
 - `oracle.webcenter.peopleconnections.wall`, the Message Board feature of the People Connections service
 - `oracle.webcenter.peopleconnections.kudos`, the Feedback feature of the People Connections service
 - `oracle.connections.community`, space membership management
- `subscription-enabled`—For specifying the default value for the preference option: `true` or `false`

Tip: Rather than enabling or disabling the entire subscription capability, the `subscription-enabled` attribute merely sets the initial state of the preference option. For example, if `subscription-enabled="true"`, then the associated subscription option is checked by default in the Spaces application's Preferences dialog. If `subscription-enabled="false"`, then the associated subscription option is not checked by default in the dialog.

- `end-user-configurable`—For enabling users to change the established default or preventing users from doing so: `true` or `false`

These attributes work together to determine the initial state of the **General Subscriptions** tab on the **Subscriptions** panel in the Spaces application's Preferences dialog ([Figure 19-1](#)).

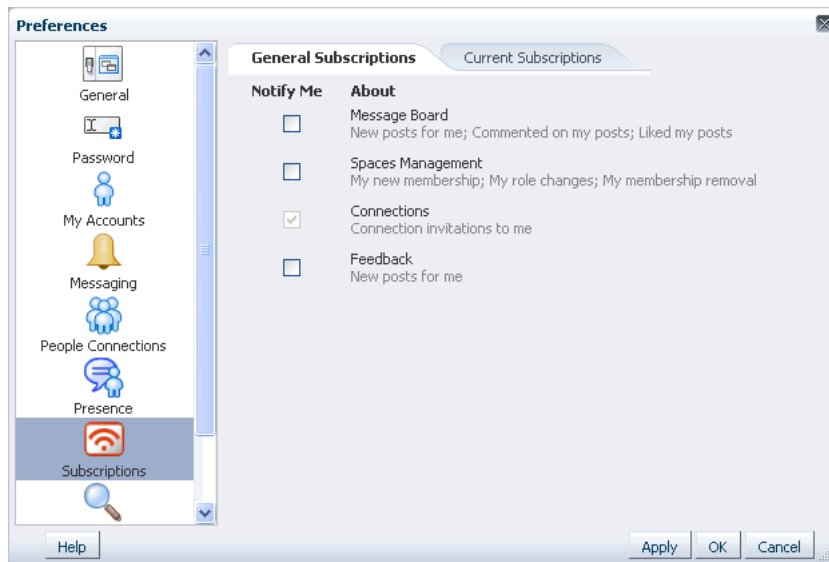
Figure 19–1 General Subscriptions Tab on the Subscriptions Panel

Table 19–1 illustrates the effect of custom administrator-level subscriptions settings on the appearance of the **General Subscriptions** tab.

Table 19–1 Effect of Administrator Defaults on Subscriptions Preferences¹

subscription-enabled ¹	end-user-configurable	Option in Preferences
True	True	Rendered normally, checkbox is checked
True	False	Grayed out, checkbox is checked
False	True	Rendered normally, checkbox is clear
False	False	Hidden, checkbox is hidden

¹ Rather than enabling or disabling the entire subscription capability, the `subscription-enabled` attribute merely sets the initial state of the preference option. For example, if `subscription-enabled="true"`, then the associated subscription option is checked by default in the Spaces application's Preferences dialog. If `subscription-enabled="false"`, then the associated subscription option is not checked by default in the dialog.

Tip: In Table 19–1, the most typical scenario for most notifications is depicted in row three.

Table 19–2 lists the types of actions that can trigger an application-level notification and associates them with their related service ID.

Table 19–2 Application-Level Activities that Can Trigger Notifications

Activity	Related Service ID
A user sends you an invitation to connect	<code>oracle.webcenter.peopleconnections.connections</code>
Your space role changes, for example, from <i>participant</i> to <i>moderator</i>	<code>oracle.webcenter.community</code>
You are added as a member of a space	<code>oracle.webcenter.community</code>
Your space membership is removed	<code>oracle.webcenter.community</code>
A user posts a message to your Message Board	<code>oracle.webcenter.peopleconnections.wall</code>

Table 19–2 (Cont.) Application-Level Activities that Can Trigger Notifications

Activity	Related Service ID
A user likes your post on another user's Message Board	oracle.webcenter.peopleconnections.wall
A user comments on your post on another user's Message Board	oracle.webcenter.peopleconnections.wall
A user posts feedback for you	oracle.webcenter.peopleconnections.kudos

19.1.2 Setting Subscription Defaults

To set defaults for application-level Subscription preferences:

1. Navigate to a directory with a path that contains `/oracle/webcenter/notification`, and create the folder `custom`.

Tip: The directory structure can start or end with any directory or directories, as long as it has `/oracle/webcenter/notification/custom` in the path.

2. In the `custom` folder, or in any subdirectory under `/oracle/webcenter/notification/custom/`, create the file `notification-service-settings.xml`.
3. In the XML file, enter values for all application-level subscription options.

[Example 19–1](#) provides sample content for an application-wide subscription preferences setting file and an example of each required option.

Example 19–1 Sample Subscriptions Settings XML File

```
<notification-service_settings xmlns="http://xmlns.oracle.com/webcenter/notification">
  <subscription-settings>
    <service id="oracle.webcenter.peopleconnections.connections" subscription-enabled="true"
      end-user-configurable="false"/>
    <service id="oracle.webcenter.peopleconnections.wall" subscription-enabled="false"
      end-user-configurable="true"/>
    <service id="oracle.webcenter.peopleconnections.kudos" subscription-enabled="false"
      end-user-configurable="true"/>
    <service id="oracle.webcenter.community" subscription-enabled="true"
      end-user-configurable="true"/>
  </subscription-settings>
</notification-service_settings>
```

Note: If an option is not provided, the default values `false/false` are assigned for the service.

4. Run the WLST command `importMetadata()`, and import the directory content into your metadata store.

See Also: For information about running WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#) For information about the `importMetadata()` command (and other WLST commands), see the section, "importMetadata," in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For example:

```
wls: /wc_domain/serverConfig> importMetadata(application='webcenter',
server='serverName', fromLocation='directoryPath', docs='/**')
```

Where:

- *application* is the name that identifies your Spaces application
- *serverName* is the name of the server on which the Spaces application is running
- *directoryPath* is the directory path under which oracle/webcenter/notification/custom/<any_sub_dir_after_this>/notification-service-settings.xml is located.

For example, if the directory path to notification-service-settings.xml is /scratch/mydir/oracle/webcenter/notification/custom, enter /scratch/mydir for *directoryPath*.

- *docs* identifies the content to be imported, in this example, the path and files that fall under *directoryPath*.

Table 19–3 describes the effect of various combinations of settings for the service ID oracle.webcenter.peopleconnections.connections.

Table 19–3 Effects of Subscription Configurations for Connections

subscription-enabled	end-user-configurable	Effect
true	true	<ul style="list-style-type: none"> ■ The subscribing user receives a notification message when another user sends the user an invitation to connect. ■ The user can change this default.
true	false	<ul style="list-style-type: none"> ■ The subscribing user receives a notification message when another user sends the user an invitation to connect. ■ The user cannot change this default.¹
false	true	<ul style="list-style-type: none"> ■ The subscribing user does not receive a notification message when another user sends the user an invitation to connect. ■ The user can change this default.
false	false	<ul style="list-style-type: none"> ■ The subscribing user does not receive a notification message when another user sends the user an invitation to connect. ■ The option for changing this default is hidden.

¹ This is the out-of-the-box default

Table 19–4 describes the effect of various combinations of settings for the service ID oracle.webcenter.peopleconnections.wall.

Table 19–4 Effects of Subscription Configurations for Message Board

subscription-enabled	end-user-configurable	Effect
true	true	<ul style="list-style-type: none"> The subscribing user receives a notification message when another user posts a message on the user's Message Board, likes the user's Message Board post, or comments on the user's Message Board post. The user can change this default.
true	false	<ul style="list-style-type: none"> The subscribing user receives a notification message when another user posts a message on the user's Message Board, likes the user's Message Board post, or comments on the user's Message Board post. The user cannot change this default.
false	true	<ul style="list-style-type: none"> The subscribing user does not receive a notification message when another user posts a message on the user's Message Board, likes the user's Message Board post, or comments on the user's Message Board post. The user can change this default.
false	false	<ul style="list-style-type: none"> The subscribing user does not receive a notification message when another user posts a message on the user's Message Board, likes the user's Message Board post, or comments on the user's Message Board post. The option for changing this default is hidden.

Table 19–5 describes the effect of various combinations of settings for the service ID `oracle.webcenter.peopleconnections.kudos`.

Table 19–5 Effect of Subscription Configurations for Feedback

subscription-enabled	end-user-configurable	Effect
true	true	<ul style="list-style-type: none"> The subscribing user receives a notification message when another user leaves feedback for the user. The user can change this default.
true	false	<ul style="list-style-type: none"> The subscribing user receives a notification message when another user leaves feedback for the user. The user cannot change this default.
false	true	<ul style="list-style-type: none"> The subscribing user does not receive a notification message when another user leaves feedback for the user. The user can change this default.
false	false	<ul style="list-style-type: none"> The subscribing user does not receive a notification message when another user leaves feedback for the user. The option for changing this default is hidden.

Table 19–6 describes the effect of various combinations of settings for the service ID `oracle.webcenter.community`.

Table 19–6 Effect of Subscription Configurations for Spaces Management

subscription-enabled	end-user-configurable	Effect
true	true	<ul style="list-style-type: none"> ■ The subscribing user receives a notification message when the user's space membership role changes, the user is added as a member of a space, or the user is removed as a member of a space. ■ The user can change this default.
true	false	<ul style="list-style-type: none"> ■ The subscribing user receives a notification message when the user's space membership role changes, the user is added as a member of a space, or the user is removed as a member of a space. ■ The user cannot change this default.
false	true	<ul style="list-style-type: none"> ■ The subscribing user does not receive a notification message when the user's space membership role changes, the user is added as a member of a space, or the user is removed as a member of a space. ■ The user can change this default.
false	false	<ul style="list-style-type: none"> ■ The subscribing user does not receive a notification message when the user's space membership role changes, the user is added as a member of a space, or the user is removed as a member of a space. ■ The option for changing this default is hidden.

19.1.3 Setting Subscriptions Preferences in Spaces

Individual users set their own subscription preferences in the Spaces application's Preferences dialog. Two Preferences panels are provided for this purpose:

- **Subscriptions**, where users subscribe to be notified about actions occurring with their space memberships and the People Connections service (Connections, Message Board, and Feedback) and view and remove their space- and object-level subscriptions
- **Messaging**, where users access controls for configuring their preferred messaging channels and filters (BPEL connection types only)

See Also: "Establishing and Managing Your Messaging Channels and Filters," and "Setting Application-Level Subscriptions," in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*

19.2 Setting Up Notifications

This section provides an overview of messaging connection types, describes prerequisites that must be in place before you can define a notification channel, and steps you through the process of setting up a notification channel for Notifications. It includes the following subsections:

- [Section 19.2.1, "What You Should Know About Connection Channels"](#)
- [Section 19.2.2, "Notification Prerequisites"](#)
- [Section 19.2.3, "Configuration Roadmap for Notifications"](#)
- [Section 19.2.4, "Specifying the Notifications Channel Using Fusion Middleware Control"](#)
- [Section 19.2.5, "Specifying the Notifications Channel Using WLST"](#)

- [Section 19.2.6, "Example - Setting Up Mail Notifications for the Spaces Application Using WLST"](#)

19.2.1 What You Should Know About Connection Channels

The Notifications connection type determines the messaging channels that are available to users when they configure their own messaging preferences for Notifications in Spaces.

Use one of two possible connection types:

- **BPEL Server** provides three messaging channel options to users: mail, texting (SMS), and worklist
- **Mail Server** delivers notification messages exclusively through a mail server that is configured for the Spaces application

BPEL Server

Selection of a BPEL server presupposes that you have established a connection with a BPEL server in which the User Messaging Service (UMS) is available. For information about connecting to a BPEL server, see [Chapter 23, "Managing the Worklist Service."](#)

When the Spaces application has `setSpacesWorkFlowConnectionName` set up, the **Manage Configuration** button becomes available on the **Messaging** panel in the Spaces application's Preferences dialog.

Tip: It is expected that the same connection you use for `setSpacesWorkFlowConnectionName` is used for Notifications, provided you use the BPEL Server for notifications.

Mail Server

Selection of a mail server presupposes that you have established a connection with a mail server. Additionally, the external application associated with the mail server connection must contain shared credentials. For information about connecting to a mail server, see [Chapter 17, "Managing the Mail Service."](#)

When **Mail Server** is the selected connection type, the **Manage Configuration** button on the **Messaging** panel in the Spaces application's Preferences dialog may or may not be grayed-out. This depends on whether you have set up `spacesWorkFlowConnection`. But, regardless, when Mail Server is the selected connection type, if clicking the **Manage Configuration** button for Messaging preferences opens User Messaging Preferences, any changes you make are ignored.

See Also: "Establishing and Managing Your Messaging Channels and Filters," in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*

19.2.2 Notification Prerequisites

Before you can define a connection type for Notifications, you must take the steps and consider the information provided in the following subsections:

- [Section 19.2.2.1, "Installation"](#)
- [Section 19.2.2.2, "Configuration"](#)
- [Section 19.2.2.3, "Security"](#)
- [Section 19.2.2.4, "Limitations"](#)

19.2.2.1 Installation

Installation requirements associated with Notifications change according to the type of connection you plan to select for Notifications messaging.

If you plan to use the User Messaging Service (UMS) through your BPEL connection for Notifications messaging, you should know that only the mail driver is installed by default. To make use of SMS and Worklist messaging channels, you must install drivers for these as well. For information about installing SMS and Worklist drivers for UMS, see the chapter "Configuring Oracle User Messaging Service," in the *Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite and Oracle Business Process Management Suite*.

If you plan to use the Mail service for Notifications messaging, no Notifications-specific installation is required, but the Mail service must be configured as described in [Chapter 17, "Managing the Mail Service."](#)

19.2.2.2 Configuration

Configuration prerequisites for Notifications also depend on the connection type you plan to select for Notifications messaging.

BPEL Server

If you plan for users to have messaging channel options—mail, texting (SMS), and Worklist—a connection to a BPEL server must be in place. Notifications uses the SOA installation for supporting multichannel notifications through the User Messaging Service (UMS). UMS is installed as a part of the SOA domain. Out of the box, only the email driver is configured. The SMS driver is available, but must be deployed. For the Worklist channel, the SOA domain must be extended through the Worklist driver extension template.

For more information see [Chapter 23, "Managing the Worklist Service,"](#) and the chapter "Configuring Oracle User Messaging Service," in the *Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite and Oracle Business Process Management Suite*.

Mail Server

If you plan that users will always and only be notified through their mail, a connection to a mail server must be in place. Additionally, the external application associated with the mail server connection must contain shared credentials. For more information, see [Chapter 17, "Managing the Mail Service."](#)

Mail notifications are sent in the preferred language specified for each user's profile. If the preferred language is not specified for a user, the server locale setting is used for mail notifications. For example, if the server is running on the Korean locale and the preferred language is not set for a user, the notification mail is in Korean.

For information about setting the preferred language, see "Choosing Your Preferred Display Language" in *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal*.

19.2.2.3 Security

There are no security considerations specifically associated with Notifications.

19.2.2.4 Limitations

UMS supports multiple messaging channels, including voice and instant messaging, that are not also supported by Notifications. From UMS, Notifications consumes only mail, SMS, and Worklist.

19.2.3 Configuration Roadmap for Notifications

Figure 19–2 and Table 19–7 provide an overview of the prerequisites and tasks required to get the Notifications service working in WebCenter Portal applications.

Figure 19–2 Configuring the Notifications Service

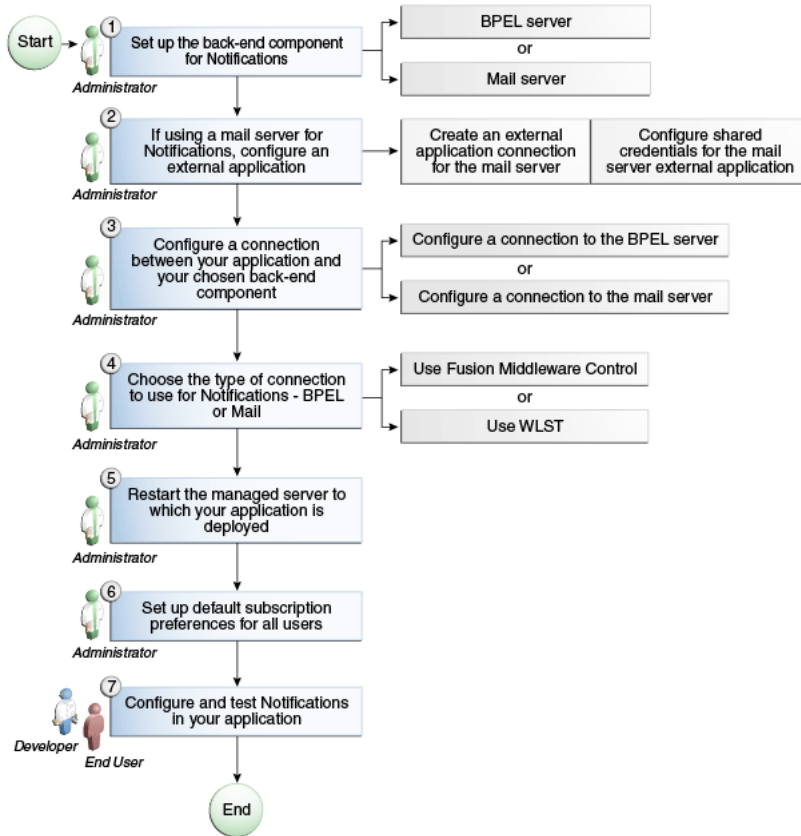


Table 19–7 Configuring Notifications

Actor	Task	Sub-task	Notes
Administrator	1. Set up the back-end component for Notifications <ul style="list-style-type: none"> Set up the BPEL server Set up the mail server 		
Administrator	2. (For mail server only) Configure an external application	<ul style="list-style-type: none"> Create an external application connection for the mail server Configure shared credentials for the mail server external application 	
Administrator	3. Create or modify a connection between your WebCenter Portal application and your chosen back-end component: <ul style="list-style-type: none"> Create a connection to the BPEL server Create a connection to the mail server 		
Administrator	4. Choose the type of connection to use for Notifications, either BPEL or Mail, by using one of the following tools: <ul style="list-style-type: none"> Fusion Middleware Control WLST 		
Administrator	5. Restart the managed server to which your application is deployed.		For the Spaces application, restart WC_Spaces. For a Framework application, restart the custom managed server where the application is deployed.
Administrator	6. Set up default subscription preferences for all users		
Developer/End User	7. Configure and test Notifications in your applications: <ul style="list-style-type: none"> Spaces application Framework applications 		

19.2.4 Specifying the Notifications Channel Using Fusion Middleware Control

To specify a Notifications message connection type with Fusion Middleware Control:

1. Log in to Oracle Fusion Middleware Control and navigate to the home page for Spaces.

For more information, see [Section 6.2, "Navigating to the Home Page for the Spaces Application."](#)

2. From the **WebCenter Portal** menu, choose **Settings > Application Configuration**.

3. On the **Application Configuration** page, scroll down to **Notifications** (at the bottom of the page), and select a connection type to use for outbound notifications: either **BPEL Server** or **Mail Server**.
4. The next step depends on the selected connection type:
If you select **BPEL Server**:
 - a. From the **Connection Name** list, select the name you provided for the BPEL server when you set up that connection.
 - b. In the **Sender Mail Address** field, enter a mail address from which all Notifications messages are sent. The sender mail address must match at least one driver that is configured to send messages from a corresponding domain.
 - c. In the **Sender SMS Address** field, enter the four- to six-digit number that is used by the User Messaging Server (UMS) as the driver from which all Notifications messages are sent. The sender SMS address must match at least one driver that is configured to send messages from a corresponding domain.If you select **Mail Server**, select a mail connection from the **Connection Name** list.
5. Save your changes.
6. Restart the managed server on which the portal application is deployed to make your configuration changes take effect.

19.2.5 Specifying the Notifications Channel Using WLST

Use the WLST command `setNotificationsConfig` to configure the connection type used for notifications. For command syntax and examples, see the section, "setNotificationsConfig," in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*. See also, "getNotificationConfig," in the same guide.

See Also: For information about how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

Note: Updates to this configuration are stored in the MDS repository. For configuration changes to take effect, you must restart the managed server on which the application is deployed. For more information, see the section, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

19.2.6 Example - Setting Up Mail Notifications for the Spaces Application Using WLST

This section provides an example of using WLST to set up Mail Notifications for the Spaces application.

In this example, we will create an external application connection, and configure shared credentials for the external application. Further, we will create a Mail connection and set Mail as the notification channel for Spaces. We will then set the subscription preferences in the Spaces application.

1. At the WLST command prompt, connect to the Administration Server for Oracle WebCenter Portal.

```
connect('admin_user','mypassword','<servername>:7001')
```

2. Create an external application connection:

```
createExtAppConnection(appName='webcenter', name='NotificationSharedApp',
displayName= 'NotificationSharedApp')
```

This command creates the connection named `NotificationSharedApp`.

3. Configure shared credentials for the external application,

`NotificationSharedApp`:

```
addExtAppCredential(appName='webcenter', name='NotificationSharedApp',
type='SHARED', username='john.doe@example.com', password='sharedpassword')
```

Where `username` refers to the email account from which email notifications will be sent. This must be in the format `<user>@<domain of the mail server>`.

Optionally, you may add the following fields that will be used while sending out the mail notification.

```
addExtAppField(appName='webcenter', name='NotificationSharedApp', fieldName='Email
Address', fieldValue='sender's_email_address', displayToUser=false)
addExtAppField(appName='webcenter', name='NotificationSharedApp', fieldName='Your
Name', fieldValue='sender's_display_name', displayToUser=false)
```

4. Create a Mail connection:

```
createMailConnection(appName='webcenter', name='NotificationSharedConn',
imapHost='<mailserver>', imapPort=143,
smtpHost='<mailserver>', smtpPort=25,
imapSecured=false, smtpSecured=false,
appId='NotificationSharedApp', default=1)
```

This creates a mail connection named `NotificationSharedConn`.

5. Set Mail as the notifications channel:

```
setNotificationsConfig(appName='webcenter', type='MAIL',
name='NotificationSharedConn')
```

This sets `NotificationSharedConn` as the mail connection to use for sending notifications.

6. For the changes to take effect, restart `WC_Spaces`, the managed server on which the Spaces application is deployed by default.**7. Log in to Spaces as a user, navigate to the **About** tab of the **Profile** page, and verify that your e-mail address is set in the **Email** field. This is to ensure that notifications are sent to the required e-mail address.**

If the e-mail address is not set, click **Edit**, then in the **Email** field, specify your e-mail address, and click **Save**.

8. Subscribe to the activities for which to receive notifications. For example, navigate to the Preferences dialog, click **Subscriptions, and then select **Space Management** to get notified about any membership or role changes.****9. Test your configuration by performing a subscribed activity. For example, change your role from Moderator to Participant to trigger a notification.**

19.3 Creating and Applying Custom Notification Templates

The notification messages that users receive through Worklist or Mail have a default format for content and content presentation. As the application administrator, you can

instead create and apply custom templates to provide your own formats for notification messages.

This section provides information about creating a custom template for notifications messages. It includes the following subsections:

- [Section 19.3.1, "What You Should Know About Overwriting Default Notification Templates"](#)
- [Section 19.3.2, "Overwriting a Default Notifications Template"](#)

19.3.1 What You Should Know About Overwriting Default Notification Templates

You can go through MDS using WLST commands to customize the layout and content of subscription-based notification messages by overwriting the files `defaultTemplate.xml` and `defaultTemplate_rtl.xml`—when right-to-left language support is required.

See Also: For information about running WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

You can create your own version of these `xml` files, editing the CSS styles for tables (`label`, `value`, `background`) and footers (`note`). You can move such tags as `<payload>` and `<group-space-footer>` to change the layout. To modify the content of these tags, you can edit the CDATA section within `<html-format>`.

Note that the tag `<text-format/>` should always be present and empty. You can use the tag `<custom>` to add additional content, where the enclosed `<html-format>` with CDATA contains the new HTML content and `<text-format/>` remains empty.

[Example 19-2](#) and [Example 19-3](#) illustrate the default content of notification message template files. You can use these to formulate your custom files.

Note: The default content of these files is very similar. The differences appear under the `<style>` tag, where alignment—either right or left—is specified.

Example 19-2 Default File `defaultTemplate.xml`

```
<?xml version="1.0"?>
<notification-template xmlns="http://xmlns.oracle.com/webcenter/notification">
  <!-- The CSS Style of the Notification -->
  <style>
    <text-format/>
    <html-format>
      <![CDATA[
        <style type="text/css">
          .title {font-size:1.2em; font-weight:bold;
            white-space:nowrap;}
          .label {text-align:right; margin-left:30px;
            padding-right:10px; white-space:nowrap;}
          .value {text-align:left; margin-right:20px;
            padding-left:10px; white-space:nowrap;
            width:100%;}
          .note {font-size:0.8em; color:#999999}
          .background {background-color:#fcfcfc}
        </style>
      ]]>
    </html-format>
  </style>
</notification-template>
```

```

        </html-format>
    </style>

    <!-- The Subject line of the Notification -->
    <subject>
        <message-key>NOTIFICATION_SUBJECT</message-key>
    </subject>
    <group-space-subject>
        <message-key>GROUP_SPACE_SUBJECT_SUFFIX</message-key>
    </group-space-subject>
    <!-- Actual srvc-specific data. Provided/Overridden by srvc template -->
    <payload>
        <text-format/>
        <html-format/>
    </payload>

    <!-- Any generic/common footer to appear after service-specific payload -->
    <!-- Group Space footer - if applicable -->
    <group-space-footer>
        <text-format/>
        <html-format>
            <![CDATA[
                <p>
                    <a href="<token>groupSpaceUrl</token>" target="_blank">
                        <message-key>GO_TO_SPACE</message-key>&nbsp;<token>
                            groupSpaceName</token>
                    </a>
                </p>
            ]]>
        </html-format>
    </group-space-footer>

    <!-- Unsubscribe footers -->
    <unsubscribe-footer>
        <text-format/>
        <html-format>
            <![CDATA[
                <hr/>
                <p class="note">
                    <token>unsubscribeMessage</token>
                </p>
            ]]>
        </html-format>
    </unsubscribe-footer>
</notification-template>

```

Example 19-3 Default File defaultTemplate_rtl.xml

```

<?xml version="1.0"?>
<notification-template xmlns="http://xmlns.oracle.com/webcenter/notification">
    <!-- The CSS Style of the Notification -->
    <style>
        <text-format/>
        <html-format>
            <![CDATA[
                <style type="text/css">
                    .title {font-size:1.2em; font-weight:bold;

```

```

        white-space:nowrap;}
        .label {text-align:left; margin-right:30px;
        padding-left:10px; white-space:nowrap;}
        .value {text-align:right; margin-left:20px;
        padding-right:10px; white-space:nowrap;
        width:100%;}
        .note {font-size:0.8em; color:#999999}
        .background {background-color:#fcfcfc}
    </style>
]]>
</html-format>
</style>

<!-- The Subject line of the Notification -->
<subject>
    <message-key>NOTIFICATION_SUBJECT</message-key>
</subject>
<group-space-subject>
    <message-key>GROUP_SPACE_SUBJECT_SUFFIX</message-key>
</group-space-subject>
<!-- Actual srvc-specific data. Provided/Overridden by srvc template -->
<payload>
    <text-format/>
    <html-format/>
</payload>

<!-- Any generic/common footer to appear after service-specific payload -->
<!-- Group Space footer - if applicable -->
<group-space-footer>
    <text-format/>
    <html-format>
        <![CDATA[
            <p>
                <a href="<token>groupSpaceUrl</token>" target="_blank">
                    <message-key>GO_TO_SPACE</message-key>&nbsp;<token>
                        groupSpaceName</token>
                </a>
            </p>
        ]]>
    </html-format>
</group-space-footer>

<!-- Unsubscribe footers -->
<unsubscribe-footer>
    <text-format/>
    <html-format>
        <![CDATA[
            <hr/>
            <p class="note">
                <token>unsubscribeMessage</token>
            </p>
        ]]>
    </html-format>
</unsubscribe-footer>
</notification-template>

```

19.3.2 Overwriting a Default Notifications Template

To overwrite an existing xml file to customize notification message formats:

1. Create a custom XML file with the name `defaultTemplate.xml` (or `defaultTemplate_rtl.xml`, for right-to-left language template).
2. Populate the custom file with your revised version of one of these default files.

See Also: [Example 19–2](#) and [Example 19–3](#) show default file content.

3. Overwrite the original file, placing the custom file where the absolute path to the file contains the namespace `oracle/webcenter/notification/custom`.

For example:

```
/tmp/repository/oracle/webcenter/notification/custom/template/defaultTemplate.xml
```

4. Upload the custom file into the WebCenter Portal's MDS repository by running the `importMetadata()` WLST command.

For example:

```
importMetadata(application='webcenter', server='WC_Spaces',
               fromLocation='template-file-location',
               docs='/oracle/webcenter/notification/custom/template/defaultTemplate.xml')
```

The `template-file-location` points to the directory under which the fully qualified custom file is located. The fully qualified custom file is typically placed under the directory structure equivalent to its namespace. For example, consider a file that is created under the following namespace:

```
/tmp/repository/oracle/webcenter/notification/custom/template/defaultTemplate.xml
```

In such a case, the `fromLocation` is `/tmp/repository` because the remaining sub-directory consists of the namespace for the XML file. The namespace must have at least the path `/oracle/webcenter/notification/custom`.

See Also: For information about the `importMetadata()` command (and other WLST commands), see the section, "importMetadata," in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

5. Restart the portal application.

19.4 Testing the Notifications Connection

In general, Notifications depends on the underlying Mail or BPEL connection to be valid when the administrator sets it. If these connections prove to be valid, then, by extension, the Notifications connections requirements are met.

Tip: For information about testing Mail connections, see [Section 17.9](#), "Testing Mail Server Connections."

19.5 Troubleshooting Issues with Notifications

Problem

No notifications are received.

Solution

- If the log indicates that the Notification Sender is not configured, then it means the service is unable to find the connection to use.
- Ensure that Notifications is configured to use either a valid BPEL or MAIL connection. This can be verified through the `getNotificationsConfig()` WLST command (see [Section 19.2.5, "Specifying the Notifications Channel Using WLST"](#)) or through the Fusion Middleware Control user interface (see [Section 19.2.4, "Specifying the Notifications Channel Using Fusion Middleware Control"](#)).

Problem

Notifications is configured (BPEL or MAIL) correctly, but still no notifications.

Solution

Notifications relies on a valid BPEL or MAIL connection. Run the respective connection validations and troubleshooting scenarios as described in [Chapter 17, "Managing the Mail Service,"](#) or [Chapter 23, "Managing the Worklist Service."](#)

Problem

MAIL or BPEL connections are set up appropriately, but still do not receive notifications.

Solution

Notifications are generated based on user subscriptions. Apart from notification for invitations to connect, which is configured out of the box, other notifications are generated only when a user has specifically subscribed. Ensure that the user has created subscriptions through his or her personal Preferences or through space- or object-level subscriptions. For more information, refer to the section, "Subscribing at the Application, space, and Object Level," in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

Problem

Users have set up their subscriptions, but still receive no notifications.

Solution

- Depending on how it is configured, Notifications delegates the delivery of notifications to BPEL/UMS or the Mail service. For the Mail service, ensure that the user's email address is configured. For UMS, look in Fusion Middleware Control under the **Message Status** section of **User Messaging Service**. Here you see the status of each outgoing message from UMS. For more information, see the chapter "Monitoring Oracle User Messaging Service," in the *Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite and Oracle Business Process Management Suite*.
- For UMS, this problem could also mean that the configuration of the sender on the WebCenter Portal side does not match or find a corresponding driver on the UMS

side. Ensure that the sender address (domain) allows UMS to match at least one driver for outbound messages.

- For the Mail service, ensure that the mail connection points to a shared connection as described in [Section 19.2.1, "What You Should Know About Connection Channels."](#)

Problem

For UMS configurations, users receive notifications on some channels but not on others.

Solution

This is most likely due to the way the user's messaging channels and filters are configured. For more information, see the section, "Establishing and Managing Your Messaging Channels and Filters," in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

Problem

For UMS configurations, only mail-channel notifications are delivered, the Worklist channel does not work.

Solution

Ensure that the SOA domain is extended with the Worklist driver template as described in the chapter "Configuring Oracle User Messaging Service," in the *Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite and Oracle Business Process Management Suite*.

Managing Personalization for WebCenter Portal

This chapter describes how to configure and manage WebCenter Portal's Personalization services.

This chapter includes the following sections:

- [Section 20.1, "What You Should Know About Personalization for WebCenter Portal"](#)
- [Section 20.2, "Before You Begin: Performing Required Configurations"](#)
- [Section 20.3, "Other Personalization Prerequisites"](#)
- [Section 20.4, "Configuring the WebCenter OPSS Trust Service"](#)
- [Section 20.5, "Configuring Providers"](#)
- [Section 20.6, "Configuring Coherence"](#)
- [Section 20.7, "Configuring Content Presenter"](#)
- [Section 20.8, "Configuring Single Sign-on"](#)
- [Section 20.9, "Overriding the Default Security Settings"](#)

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."](#)

20.1 What You Should Know About Personalization for WebCenter Portal

Personalization for WebCenter Portal provides a dynamically derived user experience for your WebCenter Portal application. Personalization evaluates defined sources of input data, generates a decision based on that evaluation, and applies this information to a declaratively defined personalization scenario. Personalization, for example, can return content or change application flow based on information about a user in a Human Resources database, targeting the application experience for that specific user.

Personalization is installed as an application in the `wc_domain` on the `wc_utilities` server. Client applications access Personalization remotely over HTTP using RESTful services. To make access easy, Java applications can use a set of provided POJO client libraries. Design-time JDeveloper tools are used to create Property Service and Conductor artifacts to be executed remotely using REST calls.

Personalization is also available in the JDeveloper integrated domain for projects that include the Personalization technology libraries when you first create your application. For evaluation purposes and iterative development, this domain offers the quickest and easiest way to explore Personalization. For more information about the Personalization architecture and services, see "Personalizing WebCenter Portal Applications" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

20.2 Before You Begin: Performing Required Configurations

The Personalization REST APIs require WebCenter Portal: Spaces. This section discusses configurations you must make to use the Personalization REST APIs.

- [Section 20.2.1, "Introduction"](#)
- [Section 20.2.2, "Configuring an Identity Asserter"](#)
- [Section 20.2.3, "Configuring the WebLogic Server Credential Store"](#)

20.2.1 Introduction

Before you can use the WebCenter Portal's Personalization REST APIs, you must perform the server-side configurations described in this section. You must perform two separate configurations. You must configure an identity asserter and you must seed required entries in the credential store, which enables the REST security tokens to function properly.

Perform these configuration tasks when WebCenter Portal: Spaces is installed for the first time or if you otherwise know the configuration tasks have not been previously performed.

For more information on security tokens, see "Security Considerations for WebCenter Portal REST APIs" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

20.2.2 Configuring an Identity Asserter

First, you must configure an identity asserter before using the REST APIs. For detailed instructions, see [Section 29.10, "Configuring the REST Service Identity Asserter."](#)

20.2.3 Configuring the WebLogic Server Credential Store

The second configuration step is to configure the WLS credential store. To configure the credential store, execute these commands while the server is running. You do not have to restart the server after executing these commands.

```
createCred(map="o.webcenter.jf.csf.map", key="keygen.algorithm",
  user="keygen.algorithm", password="AES")
createCred(map="o.webcenter.jf.csf.map", key="cipher.transformation",
  user="cipher.transformation", password="AES/CBC/PKCS5Padding")
```

20.3 Other Personalization Prerequisites

This section describes the system requirements and dependencies for Personalization in the following sections:

- [Section 20.3.1, "Personalization Installation Requirements"](#)
- [Section 20.3.2, "Personalization Configuration Requirements"](#)

- [Section 20.3.3, "Personalization Security"](#)
- [Section 20.3.4, "Personalization Limitations"](#)
- [Section 20.3.5, "Personalization Configuration Options"](#)

20.3.1 Personalization Installation Requirements

If you are using the CMIS or Activity Graph data providers, or the People Connection locator within a Personalization Conductor scenario, then WebCenter Portal: Spaces must be installed. For High Availability environments only, Coherence is also required.

20.3.2 Personalization Configuration Requirements

If you are using the CMIS provider, Activity Graph provider, PeopleConnections locator, or custom providers you must configure them as shown in [Section 20.5, "Configuring Providers."](#)

If you are using Content Presenter to present content in the Spaces application or in your Framework application, then you must also configure Content Presenter to display the results of your scenarios as described in [Section 20.7, "Configuring Content Presenter."](#)

Personalization relies on Trust Services to provide single sign-on (SSO) between different managed servers within the WebCenter Portal domain. Trust Services must be configured using the WLST scripts `configureTrustWCPS.py` and `configureConnectionsWCPS.py` provided in the `user_projects/applications/wc_domain` directory. For JDeveloper's integrated domain, only a single script (`configureWCPS.py`) located in the `DefaultDomain/scripts-wcps` directory is used. For more information about configuring Trust Services and single sign-on using this script see [Section 20.8, "Configuring Single Sign-on."](#)

20.3.3 Personalization Security

Personalization is compatible with whatever source of user authentication services are configured within the WLS security realm. That is, it can use the default identity store and policy and credential store for the domain.

If you are using the People Connections locator or Activity Graph data providers, users must also be configured as WebCenter Portal: Spaces users.

Personalization REST services are accessed through a pre-configured Personalization Web application that requires authenticated access for all resources (all URIs), with the exception of the `resourceIndex`. You can modify these constraints to provide either less security to execute scenarios (where anonymous access is needed), or more security to prevent the ability to create new scenarios. For information about modifying the default security settings, see [Section 20.9, "Overriding the Default Security Settings."](#)

In WebCenter Portal, Trust Services provides single sign-on for Personalization REST calls. This requires that the WLS `TrustServicesIdentityAsserter` is configured (it is not pre-configured). You can do this manually using the WLS Console or with the provided WLST scripts `configureTrustWCPS.py` and `configureConnectionsWCPS.py` located in the `user_projects/applications/wc_domain` directory. For JDeveloper's integrated domain, a single script (`configureWCPS.py`) located in the `DefaultDomain/scripts-wcps` directory is used.

You can also optionally secure your WebCenter Portal application's connection to the Personalization server and Personalization providers with single sign-on. For more information about configuring single sign-on, see section [Section 20.8, "Configuring Single Sign-on."](#) Access to Property Service data can also be limited by an application using a filter (IPropertyPermission) to pre-authorize access to property data.

Scenarios can use an out-of-the-box function library supporting basic Role evaluation and testing to authorize access to scenarios.

20.3.4 Personalization Limitations

By default, Personalization uses a managed server-scoped cache, meaning any changes made to cached data outside the managed server will not be seen by additional installations of Personalization.

For clustered (multiple) deployments of Personalization, Coherence may be configured for a cluster-aware cache.

20.3.5 Personalization Configuration Options

This section describes the out-of-the-box providers and other optional extensions to Personalization for WebCenter Portal, and the configuration required to integrate them into your Personalization project.

The out-of-the-box Personalization data providers allow you to write scenarios and access profile data based on existing WebCenter Portal services. These WebCenter Portal services expose their data via RESTful web services. The Personalization data providers act as REST clients of these web services and make it easy to author scenarios within JDeveloper based on these external data sources. You can also provide your own data provider and property locator implementations to integrate your own sources of external data.

CMIS Provider

The CMIS provider is an out-of-the-box provider that you can optionally use as a data source in your Personalization project. WebCenter Portal content services are exposed using the CMIS (Content Management Interoperability Services) standard. The CMIS REST service runs on the `WC_Spaces` server and provides access (based on separate configuration choices) to Oracle WebCenter Content Server.

If a Personalization user is also a Spaces user, access to user content stored through the Spaces application is possible from a scenario. For more information about Content Server see [Chapter 11, "Managing Content Repositories."](#) For more information about configuring the CMIS provider, see [Section 20.5.2, "Configuring the CMIS Provider."](#)

Activity Graph Data Provider

The Activity Graph data provider is an out-of-the-box provider that you can optionally use as a data source in your Personalization project. Activity stream information from a WebCenter Portal application is exposed through the Activity Graph service. The Activity Graph REST service runs on the `WC_Spaces` server and provides access to activity stream based recommendations as formed by the activity graph.

If a Personalization user is also a Spaces user, access to activity related recommendations (for Spaces content-types) is possible from a scenario. For more information about the Activity Graph service, see [Chapter 12, "Managing the Activity Graph Service."](#) For more information about configuring the Activity Graph provider, see [Section 20.5.3, "Configuring the Activity Graph Provider."](#)

Oracle People Connections Locator

The People Connections locator is a locator that you can optionally use as a data source in your Personalization project. People Connections service information is exposed through the People web service. The People Connection REST service runs on the WC_Spaces server and provides access to social profile data as created in the context of the Spaces application. If a Personalization user is also a Spaces user, access to People profile data is possible from a scenario. For more information about the People Connections service, see the chapter on "Integrating the People Connections Service" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

Unlike the other out-of-the-box data providers, the People Connection web service is accessed through the general purpose Property Service data provider using the IPropertyLocator extension interface. For more information about configuring the People Connections provider, see [Section 20.5.4, "Configuring the Oracle People Connections Locator."](#)

20.4 Configuring the WebCenter OPSS Trust Service

Personalization leverages a new feature from OPSS (Oracle Platform Security Services) for single-sign-on. Enabling this feature by following the configuration steps described here, is required in all but the simplest Personalization use cases.

The OPSS Trust Service does not need to be configured when:

- Directly interacting with the Conductor and Property service from a REST client
- The Conductor and Property Service are being used by Personalization client libraries from a custom JEE Web application deployed in the same domain as Personalization, if JSessionId has been configured for both Web applications (note that there will be many exceptions logged making debugging difficult)

The OPSS Trust Service must be configured when:

- Any production deployment of Personalization
- Any Personalization scenarios require the out-of-the-box data providers (Activity Graph, CMIS, and People Connections Locator)
- The Conductor and Property Service are being used by Personalization client libraries from a custom JEE Web application deployed in the same domain as Personalization
- Cross-domain trust (i.e., integrated domain connection configured to use the WC_domain CMIS provider) is required

This section contains the following subsections:

- [Section 20.4.1, "Configuring the Trust Service in the WebCenter Portal Domain"](#)
- [Section 20.4.2, "Configuring the Trust Service in the Integrated WLS Domain"](#)
- [Section 20.4.3, "Configuring Cross-Domain Trust"](#)

20.4.1 Configuring the Trust Service in the WebCenter Portal Domain

The default WebCenter Portal installation includes the Personalization domain extension template, which installs two WLST python scripts (`configureTrustWCPS.py` and `configureConnectionsWCPS.py`), in the domain home:

```
oracle/user_projects/applications/wc_domain/scripts
```

These scripts and associated `configureWCPS.properties` file contain usage instructions. Note that these are sample scripts, and that before running the scripts, you must edit the properties file and, at a minimum, specify the `ocs.server` name (typically the Content Server), the `spaces.server.host` name, and the `fmwconfig.location`. These values are unique to each WebCenter Portal installation and must be edited. Other values may also need to be changed according to the local environment (the machine port numbers, for example, may be different).

The `configureConnectionsWCPS.py` script sets up the default Personalization connection information for you (i.e., connection information for Activity Graph, CMIS, and People Connections). The script relies on the `WCPS.py` library, which is only installed on the WebCenter Portal domain (and not in the integrated WLS domain). You can, however, run `configureConnectionsWCPS.py` in the WebCenter Portal domain and point it (using a t3 URL) to an integrated WLS domain.

Caution: the Trust Service configuration set up by `configureTrustWCPS.py` should not be applied remotely. The script should only be run from the WebCenter Portal domain (`wc_domain`).

You must use the `oracle/as11gr1wc/common/bin/wlst.sh` command file that sets up environment variables correctly (for `as11gr1wc` scripts).

After running the scripts, restart all servers in the domain.

Testing the Configuration

To see Trust Service single sign-on in operation, you must be calling the Conductor or Property Service from a custom JEE Web application (using the Personalization client libraries), or be executing a scenario that uses a Personalization connection (such as the Activity Graph or CMIS data providers), or accessing a People Connections property using the People Connections locator.

When doing any of the above, you should see the following default log entry in `WC_Uutilities-diagnostic.log`:

```
[2010-11-10T07:30:40.362-08:00] [WC_Uutilities] [NOTIFICATION] []
[oracle.jps.trust] [tid: [ACTIVE].ExecuteThread: '3' for queue:
'weblogic.kernel.Default (self-tuning)']
[ecid: 0000IkqQG4NBh49LJeCCyf1CqfXw000008,0] [APP: wcps-services#11.1.1.4.0] Token
issue operation
```

You should also see the following default log entry in the `WC_Spaces-diagnostic.log` (if accessing services there):

```
[2010-11-10T07:30:40.236-08:00] [WC_Spaces] [NOTIFICATION] [] [oracle.jps.trust]
[tid: [ACTIVE].ExecuteThread: '1' for queue: 'weblogic.kernel.Default
(self-tuning)']
[ecid: d461d36d4a552b90:-1fe62a5d:12c365bb19b:-8000-000000000000002c,0] [APP:
webcenter#11.1.1.4.0] Token validate operation.
```

20.4.2 Configuring the Trust Service in the Integrated WLS Domain

A separate python script is shipped with the JDeveloper installer to configure the integrated WLS domain located in the following directory:

```
DefaultDomain\scrpts-wcps\
```

This script can be run manually or using JDeveloper's **Run External Script** function.

Edit the properties file if you are using a non-default user or password. After creating and starting the integrated WLS domain, run the script from the `scripts-wcps` directory:

```
Oracle\MiddlewareRC8\oracle_common\common\bin\wlst.cmd configureWCPS.py
configureWCPS.properties
```

Restart the integrated WLS domain.

Testing the Configuration

Default logging levels are not enough to confirm token-issue and token-validate operations. Use the **Configure Oracle Diagnostic Logging** feature in JDeveloper and navigate to the `oracle.jps.trust` logger and set the level to `Finest`. Now run a scenario involving a custom JEE Web application calling the Conductor or Property Services.

20.4.3 Configuring Cross-Domain Trust

The Trust Service supports cross-domain trust, meaning if keystores have been created in different WLS domains, a client may allocate a token in domain 'A', issue an HTTP request with the token to domain 'B', and have the identity asserter validate and authenticate the user/request in domain 'B' through single sign-on. Note that a key assumption is that the user in domain 'A' exists in, and is the same user in domain 'B'.

By default, when running the `configureWCPS.py` script in the integrated WLS domain a certificate named `extDomain.cer` is generated. To enable cross-domain trust between the integrated WLS domain and WebCenter Portal domain:

Copy `extDomain.cer` to your WebCenter Portal domain (`wc_domain`) installation and import it there. Copy the `extDomain.cer` file to the `scripts` location:

```
oracle/user_projects/applications/wc_domain/scripts
```

Type in the following command to import the certificate:

```
keytool -importcert -alias orakey1 -file extDomain.cer -keystore
../../../../wlsserver_10.3/wc_domain/config/fmwconfig/default-keystore.jks
-storepass weblogic
```

Restart the servers in the WebCenter Portal domain.

Testing the Configuration

The simplest way to validate cross domain trust is to create a People Connections Personalization connection in the integrated WLS domain that points to the WebCenter Portal domain's `WC_Spaces` server. Then, create and deploy a simple scenario to the integrated WLS domain that fetches a People Connections property value. Finally, confirm that the 'Token Validate Operation' message described above is logged on the `WC_Spaces` server.

20.5 Configuring Providers

Personalization for WebCenter Portal provides out-of-the-box providers for Activity Graph and the Content Server, and a locator for People Connections. For scenarios using any of these providers, you must configure them using the `configureWCPY.py` WLST script as described in the following sections. If you are using custom providers or locators, then you must also configure them as described in

the section on configuring custom providers. You do not need to configure providers or locators if they are not being used in your scenarios.

You can develop scenarios without the out-of-the-box providers, or exclusively with custom providers or downloaded from OTN. Also, if you are developing exclusively within the JDeveloper integrated domain, you do not ordinarily have access to these WC_Spaces-based services (since WebCenter Portal: Spaces does not run in the integrated domain). With advanced configurations (also supported by `configureWCPS.py`) you can access the WebCenter Portal: Spaces services in the WC_Spaces domain from the integrated domain's Personalization server. This uses cross-domain trust and does require the provider connections to be configured.

The `configureTrustWCPS.py` and `configureConnectionsWCPS.py` scripts (located in the WC_Spaces domain), or `configureWCPS.py` for JDeveloper's integrated WLS domain (located in the `DefaultDomain/scripts-wcps` domain directory) are used to configure the corresponding domains by pointing to the appropriate WLS Administration server.

- [Section 20.5.1, "Creating or Modifying Provider Connection Settings"](#)
- [Section 20.5.2, "Configuring the CMIS Provider"](#)
- [Section 20.5.3, "Configuring the Activity Graph Provider"](#)
- [Section 20.5.4, "Configuring the Oracle People Connections Locator"](#)
- [Section 20.5.5, "Configuring Custom Providers"](#)

20.5.1 Creating or Modifying Provider Connection Settings

This section describes how to use WLST, JConsole, Fusion Middleware Control to create or change the connection information stored in `wcps-connections.xml`. It also describes how you can write a custom configuration class to configure a custom provider.

This section contains the following subsections:

- [Section 20.5.1.1, "Understanding Personalization Connection Information"](#)
- [Section 20.5.1.2, "Connection Configuration Attributes"](#)
- [Section 20.5.1.3, "Configuring Connections Using WLST"](#)
- [Section 20.5.1.4, "Configuring Connections Using JConsole"](#)
- [Section 20.5.1.5, "Configuring Connections Using Fusion Middleware Control"](#)
- [Section 20.5.1.6, "Writing a Custom Configuration Class"](#)

20.5.1.1 Understanding Personalization Connection Information

Personalization connection information is maintained in `wcps-connections.xml`, which can be found in the domain directory at the following location:

```
<domain directory>/config/fmwconfig/wcps-connections.xml
```

Although editing this file directly is not recommended, there are several ways in which you can modify connection information:

- WLST - you can write a script with WLST commands to access the system MBeans representing the connection configuration. For more information on using WLST commands to configure connection settings, see [Section 20.5.1.3, "Configuring Connections Using WLST."](#)

- JConsole - you can use JConsole to view or edit connection configuration by creating or editing connection JMX MBeans. For more information on using JConsole to configure connection settings, see [Section 20.5.1.4, "Configuring Connections Using JConsole."](#)
- Fusion Middleware Control - you can use Fusion Middleware Control to view or edit the JMX MBeans deployed with Personalization. For more information on using Fusion Middleware Control to configure connection settings, see [Section 20.5.1.5, "Configuring Connections Using Fusion Middleware Control."](#)

20.5.1.2 Connection Configuration Attributes

The following shows the connection properties and attributes (maintained in `wcps-connections.xml`) that can be modified using WLST, JConsole, or Fusion Middleware Control. Note that each connection property is specific to the provider or locator that the connection is for. For example, the CMIS provider will have different connection properties than the Activity Graph provider.

- **<connection-name>** - unique name for this connection. Connections can be retrieved by name.
- **<connection-type>** - unique type for this connection. Connections can be retrieved by type. Note that `connection-type` only needs to be specified for custom connections. For the out-of-the-box data providers this field is set internally.
- **<namespace>** - generally, this must match the namespace the accessing scenario is deployed within. The namespace is how the Conductor determines how to locate the appropriate `<connection>` for a given scenario. You can use a wildcard `*` to make this connection element available in all namespaces. If left unspecified in the WLST script, `namespace` will default to `'*`.
- **<name>isDefault</name>** - marks this connection as the default connection (if multiple are defined). Note that multiple connections can have the "isDefault" flag set to true. If this is the case, it is up to the individual provider to return the default connection.

20.5.1.3 Configuring Connections Using WLST

A set of Personalization WLST commands is provided to allow easy configuration of your provider connections. You can combine these commands into a script, an example of which that can be customized or used directly is provided. The sample script sets up provider connections and also initializes the Trust Services.

The Personalization WLST commands are installed at `oracle/as11gr1wc/common/wlst/WCPS.py` and are invoked using the `oracle/as11gr1wc/common/bin/wlst.sh(cmd)` script.

Each out-of-the-box data provider is supported with specific WLST commands (described in sections below). For custom data providers, use the generic WLST commands to configure a connection. For example:

```
createWCPSCustomConnection('customConnectionName',
'connectionType', properties={ 'name1': 'value1', 'name2':
'value2' })
```

For a complete list of Personalization WLST connection and other commands, see the section "Personalization" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

20.5.1.4 Configuring Connections Using JConsole

JConsole (located in `$JAVA_HOME/jdk6/bin/jconsole`), can be used to create, view or edit the JMX MBeans (the connection configuration MBeans for Activity Graph, CMIS, and People Connections) deployed with Personalization for WebCenter Portal. These tasks are described in the following subsections:

- [Section 20.5.1.4.1, "Creating a New Connection Using JConsole"](#)
- [Section 20.5.1.4.2, "Editing Connection Settings Using JConsole"](#)

20.5.1.4.1 Creating a New Connection Using JConsole

To create a connection:

1. Invoke JConsole as shown below:

```
jconsole
-J-Djava.class.path=$JAVA_HOME/lib/jconsole.jar:$JAVA_HOME/lib/tools.jar:$ORACLE_HOME/oracle/wlserver_10.3/server/lib/wljmxclient.jar
-J-Djmx.remote.protocol.provider.pkgs=weblogic.management.remote
```

2. Open the JConsole Remote Connection:

```
service:jmx:iiop://example.com:7001/jndi/weblogic.management.mbeanservers.domainruntime
Username: weblogic
Password: welcome1
```

3. In the tree under `oracle.wcps.connections`, navigate to **ConnectionConfiguration** and select **Operations**.
4. Click **addConnection** and enter the **Namespace**, **Type**, and **Name**.

Note that these connections are predefined for the out-of-the-box providers by using the `configureConnectionsWCPS.py` script.

20.5.1.4.2 Editing Connection Settings Using JConsole

To view or edit connection settings:

1. Invoke JConsole as shown below:

```
jconsole
-J-Djava.class.path=$JAVA_HOME/lib/jconsole.jar:$JAVA_HOME/lib/tools.jar:$ORACLE_HOME/oracle/wlserver_10.3/server/lib/wljmxclient.jar
-J-Djmx.remote.protocol.provider.pkgs=weblogic.management.remote
```

2. Open the JConsole Remote Connection:

```
service:jmx:iiop://example.com:7001/jndi/weblogic.management.mbeanservers.domainruntime
Username: weblogic
Password: welcome1
```

3. Change the connection property for the provider. For example, to change the Activity Graph host name:

- a. Expand the tree:

```
oracle.wcps.connections->ConnectionConfiguration.Namespace.Connection->default->activity.provider.connection->ConnectionConfiguration->wcps-services->ActivityGraphConfigConnection->Attributes
```

- b. Click on **Properties**.

- c. In the right panel, double click the value in the first row.
You can now scroll through current values using **Composite Navigation**.
- d. To change the host value, click on **Properties** in the navigation tree, supply a name and new value, and then click **setProperty**.

20.5.1.5 Configuring Connections Using Fusion Middleware Control

You can use Fusion Middleware Control to view or edit the JMX MBeans (the connection configuration MBeans for Activity Graph, Content Server, and People Connections deployed with Personalization for WebCenter Portal).

To view or edit connection configuration MBeans:

1. Open Fusion Middleware Control Navigate to **Personalization Services**.
2. Click **WCPS-Services**.
3. From the Application Development drop-down menu, select **System MBean Browser**.
4. In the MBean browser under 'Application Defined MBeans', select `oracle.wcps.connections` and continue to drill down to the connection information you wish to modify.
5. On the Attributes tab, select **Properties** to view current values of connection attributes.
6. On the Operations tab, select **setProperty** and click **Invoke** to modify the name/value pairs.

20.5.1.6 Writing a Custom Configuration Class

Custom configuration classes (classes annotated with `@ConnectionConfiguration`) are implemented by customers writing their own data providers. This allows custom data providers to use the Personalization connection framework to retrieve connection information configured using the Personalization WLST scripts.

Custom configuration classes for data providers are more fully described in the section on "Custom Data Providers" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

20.5.2 Configuring the CMIS Provider

If you are working outside of the Integrated WLS domain (i.e., in the `WC_Spaces` domain), before you can use the CMIS provider in your scenario, you must first configure connection settings for it.

Connection settings for the CMIS provider are maintained in `wcps-connections.xml` in the `wc_domain` conductor extensions directory (domain scoped). Although it is not recommended that you edit this file directly, there are several other ways in which you can modify connection settings. Use one of the methods described in [Section 20.5.1, "Creating or Modifying Provider Connection Settings."](#) to configure the connection settings for the CMIS provider.

Connection Element and Property Descriptions

<connection-name> - unique name for this connection. Connections can be retrieved by name.

<namespace> - generally, this must match the namespace the accessing scenario is deployed within. The namespace is how the Conductor determines how to locate the appropriate **<connection>** for a given scenario. Using a wildcard '*', you can make this connection element available in all namespaces.

<name>isDefault</name> - marks this connection as the default connection (if multiple connections are defined)

<name>repositoryId</name> - this property must be changed to match the Content Repository in your environment.

<name>path</name> - this property must be changed to match the Content Repository in your environment. Defaults to `/api/cmisis/repository/repositoryId` if not specified

<name>scheme</name> - protocol to access the CMIS REST service (HTTP or HTTPS for SSL). Defaults to HTTP if not explicitly specified.

<name>host</name> - machine name hosting the CMIS REST service. This is the machine name of the WC_Spaces managed server.

<name>port</name> - machine port number hosting the CMIS REST service. This is the machine port number of the WC_Spaces managed server.

<name>pathTrim</name> - Default is no trim if not explicitly specified

<name>rewriteUrls</name> - can be set to `None`, `Consumer`, or `Producer`. See the REST Proxy page for details. If you want the direct URLs (from the CMIS server for document links), set this to `None`. Default is no rewrite (`None`).

<name>username</name> - (Optional) the username to use when connecting to the CMIS REST service. Can be used to force a connection to a fixed username.

<name>password</name> - (Optional) the password to use when connecting to the CMIS REST service. Used in conjunction with `username`, can be used to force a connection to a fixed username/password. Not recommended for use outside of development environment since password access is not secured.

<name>timeoutInMillisecs</name> - Time in milliseconds before the CMIS query read response times out

<name>propagateTimeoutExceptions</name> - If true, propagate the timeout exceptions. Otherwise, log the exception and return null for the CMIS query response.

20.5.3 Configuring the Activity Graph Provider

If you are working outside of the Integrated WLS domain (i.e., in the WC_Spaces domain), before you can use scenarios that rely on the Activity Graph provider, you must configure connection information for your local environment.

Connection settings for Activity Graph are maintained in `wcps-connections.xml` in the `wc_domain` conductor extensions directory (domain scoped). Although it is not recommended that you edit this file directly, there are several other ways in which you can modify connection settings. Use one of the methods described in [Section 20.5.1, "Creating or Modifying Provider Connection Settings."](#) to configure the connection settings for the Activity Graph provider.

Connection Element and Property Descriptions

<connection-name> - unique name for this connection. Connections can be retrieved by name.

<namespace> - generally, this must match the namespace the accessing scenario is deployed within. The namespace is how the Conductor determines how to locate the appropriate `<connection>` for a given scenario. Using a wildcard '*', you can make this connection element available in all namespaces.

<name>isDefault</name> - marks this connection as the default connection (if multiple connections are defined)

<name>scheme</name> - protocol to access the CMIS REST service (HTTP or HTTPS for SSL). Defaults to HTTP if not explicitly specified.

<name>host</name> - machine name hosting the Activity Graph REST service. This is the machine name of the WC_Spaces managed server.

<name>port</name> - machine port number hosting the Activity Graph REST service. This is the machine port number of the WC_Spaces managed server.

<name>rewriteUrls</name> - can be set to `None`, `Consumer`, or `Producer`. See the REST Proxy page for details. If you want the direct URLs (from the CMIS server for document links), set this to `None`. Default is no rewrite (`None`).

<name>user</name> - (Optional) the username to use when connecting to the Activity Graph REST service.

<name>password</name> - (Optional) the password to use when connecting to the Activity Graph REST service. Used in conjunction with `username`, can be used to force a connection to a fixed username/password. Not recommended for use outside of development environment since password access is not secured.

<name>restResourceIndex</name> - the URI suffix to append to the host/port for the REST resource index (for example: '/rest/api/resourceIndex')

20.5.4 Configuring the Oracle People Connections Locator

If you are working outside of the Integrated WLS domain (i.e., in the WC_Spaces domain), before you can use scenarios that rely on the People Connections locator, you must configure connection information for your local environment.

The Property Service uses an `IPropertyLocator` (the People Connections `ILocator`) to interface with the People Connections service. The Property Provider that interfaces with the People Connections service uses this `ILocator` to make PC REST calls for a given user (or self) and return the 'Person' object represented by that REST service call. The Person attributes represent values for that WebCenter Portal profile.

Connection settings for the People Connections `ILocator` are maintained in `wcps-connections.xml` in the `wc_domain` conductor extensions directory (domain scoped). Although it is not recommended that you edit this file directly, there are several other ways in which you can modify connection settings. Use one of the methods described in [Section 20.5.1, "Creating or Modifying Provider Connection Settings."](#) to configure the connection settings for the People Connections `ILocator`.

Connection Element and Property Descriptions

<connection-name> - unique name for this connection. Connections can be retrieved by name.

<namespace> - generally, this must match the namespace the accessing scenario is deployed within. The namespace is how the Conductor determines how to locate the appropriate `<connection>` for a given scenario. Use a wildcard '*' to make this connection element available in all namespaces.

<name>isDefault</name> - marks this connection as the default connection (if multiple are defined)

<name>scheme</name> - protocol to access the CMIS REST service (HTTP or HTTPS for SSL). Defaults to HTTP if not explicitly specified.

<name>host</name> - machine name hosting the PC REST service. This is the machine name of the WC_Spaces managed server.

<name>port</name> - machine port number hosting the PC REST service. This is the machine port number of the WC_Spaces managed server.

<name>user</name> - (Optional) the username to use when connecting to the People Connection REST service. Can be used to force a connection to a fixed username.

<name>password</name> - (Optional) the password to use when connecting to the People Connections REST service. Used in conjunction with `username`, can be used to force a connection to a fixed username/password. Not recommended for use outside of development environment since password access is not secured.

<name>restResourceIndex</name> - appended to the PC REST service host/port, pointing to the location of the `resourceIndex` (available REST services) page (for example: `/rest/api/resourceIndex`)

Bootstrapping the Person class to the Properties Provider

In order for the Property Service to know about and use the results of the People Connections REST calls, it needs to know about a 'Person'. This means creating a 'Person' property set definition, along with its individual attributes set as property definitions, before a 'Person' can be instantiated and its properties set.

The People Connection ILocator code does this by bootstrapping that process in a servlet listener, configured in its `web.xml` file as shown in the example below:

```
<?xml version="1.0" encoding="UTF-8" ?>
<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee
http://java.sun.com/xml/ns/j2ee/web-app_2_4.xsd"
version="2.4">

    <!-- Allows connection config classes to be loaded from the connections.xml
file -->
    <listener>

<listener-class>oracle.wcps.connection.lifecycle.VersatileModuleLifecycleCallback<
/listener-class>
    </listener>

    <listener>

<listener-class>oracle.wcps.people.util.BootstrapPropertiesListener</listener-clas
s>
    </listener>

</web-app>
```

Accessing the PC REST connection configuration information

Because the People Connections ILocator is not an actual 'provider', you cannot access its connection information in provider code, as for example Activity Graph. Instead,

internal code uses the `VersatileModuleLifecycleCallback` class to make that configuration information available, and consequently makes this a required listener to be configured in `web.xml`. Once that listener has been activated, the code can make calls to access connection information and parameterize the `ILocator` code to point to the PC REST server.

Tying the PC ILocator to the Properties Service Provider

The Properties Service Provider (PSP) knows about the People Connections ILocator through the namespaces. In the bootstrapping process above, the `PropertySetDefinition` (and its definitions) are namespaced with "people.connections.person" and a locator class "oracle.wcps.people.property.PeoplePropertyLocator". In using the PSP, the namespace and `PropertySetDefinition` are passed to the PSP. The PSP uses the locator class defined in the `PropertySetDefinition` to instantiate and delegate to property values (Person values from the People Connections REST service).

The locator and namespaces are critical in this process. They are defined as constants in the internal `PropertyDefConstants` class. Note that these do not need to be configured.

20.5.5 Configuring Custom Providers

Connection settings for Activity Graph are maintained in `wcps-connections.xml` in the `wc_domain` conductor extensions directory (domain scoped). Although it is not recommended that you edit this file directly, there are several other ways in which you can modify connection settings. Use one of the methods described in [Section 20.5.1, "Creating or Modifying Provider Connection Settings."](#) to configure the connection settings for your custom provider. Refer to [Section 20.5.1.2, "Connection Configuration Attributes"](#) for information about the configuration file elements and property descriptions.

20.6 Configuring Coherence

If your installation is using Coherence for caching (a requirement for "high-availability" environments), four separate caches must be set up: one each for Namespaces, Property Definitions, Property Set Definitions, and Property Sets.

The sample `wcps-cache-config.xml` configuration file below shows how to configure simple Coherence local caches. For more advanced cache types, refer to the Coherence documentation. Note that Coherence classes must be accessible via the same class loader as Personalization. The `wcps-cache-config.xml` file must also be accessible by that same class loader. For more information, see the `oracle.wcps.cache.CacheFactory` class in the JavaDoc for WebCenter Portal in the *Oracle Fusion Middleware Java API Reference for Oracle WebCenter Portal*.

```
<?xml version="1.0" encoding="UTF-8" ?>
<cache-config>
  <caching-scheme-mapping>
    <cache-mapping>
      <cache-name>com.oracle.p13n.service.property.namespaces</cache-name>
      <scheme-name>ns-local-side</scheme-name>
    </cache-mapping>
    <cache-mapping>
      <cache-name>com.oracle.p13n.service.property.propertydefinitions_*</cache-name>
      <scheme-name>pd-local-side</scheme-name>
    </cache-mapping>
  </caching-scheme-mapping>
</cache-config>
```

```

    <cache-mapping>
<cache-name>com.oracle.p13n.service.property.propertysetdefinitions_*</cache-name>
    <scheme-name>psd-local-side</scheme-name>
</cache-mapping>
<cache-mapping>

<cache-name>com.oracle.p13n.service.property.propertysets_*</cache-name>
    <scheme-name>ps-local-side</scheme-name>
</cache-mapping>
<cache-mapping>
    <cache-name>*</cache-name>
    <scheme-name>properties-default-local</scheme-name>
</cache-mapping>
</caching-scheme-mapping>

<caching-schemes>
<!--
The following schemes are all local. For a clustered deployment,
a distributed, replicated, or other clustered scheme is recommended.
See Coherence documentation for more information.
-->

    <local-scheme>
        <scheme-name>ns-local-side</scheme-name>
        <service-name>NamespaceCache</service-name>

        <eviction-policy>HYBRID</eviction-policy>
        <high-units>{back-size-limit 0}</high-units>
        <unit-calculator>FIXED</unit-calculator>
        <expiry-delay>{back-expiry 1h}</expiry-delay>
        <flush-delay>1m</flush-delay>

        <cachestore-scheme/>
    </local-scheme>

    <local-scheme>
        <scheme-name>pd-local-side</scheme-name>
        <service-name>PropertyDefinitionCache</service-name>

        <eviction-policy>HYBRID</eviction-policy>
        <high-units>{back-size-limit 0}</high-units>
        <unit-calculator>FIXED</unit-calculator>
        <expiry-delay>{back-expiry 1h}</expiry-delay>
        <flush-delay>1m</flush-delay>

        <cachestore-scheme/>
    </local-scheme>

    <local-scheme>
        <scheme-name>psd-local-side</scheme-name>
        <service-name>PropertySetDefinitionCache</service-name>

        <eviction-policy>HYBRID</eviction-policy>
        <high-units>{back-size-limit 0}</high-units>
        <unit-calculator>FIXED</unit-calculator>
        <expiry-delay>{back-expiry 1h}</expiry-delay>
        <flush-delay>1m</flush-delay>

        <cachestore-scheme/>

```

```

</local-scheme>

<local-scheme>
  <scheme-name>ps-local-side</scheme-name>
  <service-name>PropertySetCache</service-name>

  <eviction-policy>HYBRID</eviction-policy>
  <high-units>{back-size-limit 0}</high-units>
  <unit-calculator>FIXED</unit-calculator>
  <expiry-delay>{back-expiry 1h}</expiry-delay>
  <flush-delay>1m</flush-delay>

  <cachestore-scheme/>
</local-scheme>

<local-scheme>
  <scheme-name>properties-default-local</scheme-name>
  <service-name>DefaultCache</service-name>

  <eviction-policy>HYBRID</eviction-policy>
  <high-units>{back-size-limit 0}</high-units>
  <unit-calculator>FIXED</unit-calculator>
  <expiry-delay>{back-expiry 1h}</expiry-delay>
  <flush-delay>1m</flush-delay>

  <cachestore-scheme/>
</local-scheme>

</caching-schemes>

</cache-config>

```

20.7 Configuring Content Presenter

Before you can run Personalization for WebCenter Portal scenarios using Content Presenter, you need to configure the connections file (`connections.xml`) so that Content Presenter can see your Conductor server and the tagged scenarios. For more information about Content Presenter, see "Publishing Content Using Content Presenter" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

The `connections.xml` file holds the connection information for the application that you're working with on the WebCenter Portal side. Content Presenter gets a list of all URL connections that are registered within this file and for any that begin with "Conductor", Content Presenter will assume this is a URL pointing to a Conductor server. For more information about `connections.xml`, see Appendix A, "Files for WebCenter Portal: Framework Applications" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

You can configure the Content Presenter task flow either at runtime, or from JDeveloper when adding the Content Presenter task flow to a page. These two configuration options for Content Presenter, as well as configuration requirements on the Conductor side are described in the following subsections:

- [Section 20.7.1, "Configuring the WebCenter Portal Application's Content Server Connection"](#)
- [Section 20.7.2, "Configuring the Content Presenter Task Flow Parameters"](#)
- [Section 20.7.3, "Configuring the Conductor's Scenario Tags"](#)

20.7.1 Configuring the WebCenter Portal Application's Content Server Connection

For a WebCenter Portal application, use JDeveloper to set up the URL connection, or set the Content Presenter task flow parameters as described in [Section 20.7.2, "Configuring the Content Presenter Task Flow Parameters."](#) For WebCenter Portal: Spaces, you can use either WLST commands or Fusion Middleware Control to configure the connection.

This section contains the following subsections:

- [Section 20.7.1.1, "Configuring Connections for the Spaces Application Using WLST"](#)
- [Section 20.7.1.2, "Configuring Connections for the Spaces Application Using Fusion Middleware Control"](#)

20.7.1.1 Configuring Connections for the Spaces Application Using WLST

For the Spaces application, you can use the `adf_createURLConnection` WLST command to manage URL connections as shown in the following example:

```
adf_createURLConnection('webcenter', 'Conductor', 'http://example.com:8891/wcps/api/conductor?namespace=CP_namespace&
```

For more information about the `adf_createURLConnection` command, see the section "adf_createURLConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

20.7.1.2 Configuring Connections for the Spaces Application Using Fusion Middleware Control

For the Spaces application, you can use Fusion Middleware Control to configure connections.

To configure connections using Fusion Middleware Control:

1. Log in to Fusion Middleware Control and navigate to the home page for the Spaces application.
See: [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
2. From the **WebCenter Portal** menu, select **ADF -> Configure ADF Connections**.
The ADF Connections Configuration page displays (see [Figure 20–1](#)).

Figure 20–1 ADF Connections Configuration Page

3. Set the **Connection Type** to `Url`, enter the **Connection Name** as `Conductor`, and click **Create Connection**.

The URL Connections section displays (see [Figure 20–2](#)).

Figure 20–2 ADF Connections Configuration Page (URL Connections)

ADF Connections Configuration ?

Use this page to add, edit or delete connections.
To create a new connection, select a Connection Type from the list below and enter a Connection Name. The Connection Configurations page updates with fields for configuring the selected connection type.

Create Connection

Connection Type:
 Connection Name:

URL Connections

Connection Name	URL
Conductor	http://www.example.com

- Click the **Edit** (Pencil) icon.
The URL Connection dialog displays (see [Figure 20–3](#)).

Figure 20–3 URL Connection Dialog

URL Connection

Specify properties for Conductor connection.

URL: Set the url for th

User Name:

Password:

Authentication Realm:

Proxy:

Proxy Use Default:

Connection Class Name:

Challenge Authentication Type:

- Edit the URL so that it points to the Content Server instance used by the Spaces application. For example:

```
http://example.com:8891/wcps/api/conductor?namespace=CP_namespace&repoId=myhost-ucm11g
```
- Update any other fields as required for your local connection and click **OK**.

20.7.2 Configuring the Content Presenter Task Flow Parameters

You can configure a Content Presenter instance through its task flow parameters. These can either be set at runtime in the Content Presenter Configuration dialog, or from JDeveloper as you add the Content Presenter task flow. To do this manually, you need to set two parameters: the `Data Source Type` parameter must be set to `dsTypeScenarioResults`, and the `Data Source` parameter should be set to something like:

```
conductor-connection-name=ConductorConnectionName,namespace=ScenarioNamespace,scenario-name=ScenarioName,inputparam1=value1,inputparam2=value2
```

Note that the `conductor-connection-name` value must match with a URL connection that points to a valid Conductor server. Also, the namespace used should

be the name of the namespace to which the specified scenario belongs. Finally, any input parameters that the scenario may be expecting can be appended (as shown above), with a comma separating the name/value pairs.

For more information about configuring Content Presenter for Personalization, see:

- At runtime: "Setting Content Presenter Task Flow Properties" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*
- In JDeveloper: "Content Presenter Task Flow Parameters and Out-of-the-Box Display Templates" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

20.7.3 Configuring the Conductor's Scenario Tags

On the Conductor side, your Scenarios must have the correct tag in order for Content Presenter to see them. Content Presenter uses the tag `ContentPresenterScenario`, so any scenarios you want Content Presenter to pick up must have this tag associated with them.

Once you have everything set up on both the Conductor and WebCenter Portal application side, everything else is fairly simple. When you open the Content Presenter Configuration dialog at runtime, the Content Source selection list displays **Results of a Scenario**. Selecting this displays a table of all of the scenarios that have been tagged for Content Presenter consumption. The first Scenario is always selected, and if it has any Input Parameters defined, they will be displayed below the table with input fields.

As you select scenarios in the table, the Input Parameters below will be updated. After selecting a scenario and specifying any input parameters, you can either preview or save Content Presenter to get the results. The results will be displayed much like any other multi-valued content source and will ultimately depend on the template selected for display purposes.

Note: Any results that are returned from a scenario for use within Content Presenter must return a valid CMIS query as Content Presenter takes the return value and runs it (as a CMIS query) against the repository specified within the Conductor URL.

20.8 Configuring Single Sign-on

Single sign-on is configured as part of running the `configureTrustWCPS.py` and `configureConnectionsWCPS.py` scripts for configuring the WebCenter Portal domain, or the `configureWCPS.py` script for configuring JDeveloper's integrated WLS domain. When you run these scripts they also set up Trust Services single sign-on, which allows single sign-on for REST HTTP requests between client JEE Web applications, the Personalization Web application, and the `WC_Spaces` Web application REST services used by the out-of-the-box data providers. All these WebCenter Portal applications are also configured to support OAM/OSSO-provided single sign-on tokens, as well, without any additional Personalization-specific configuration. For more information, see [Section 20.4.3, "Configuring Cross-Domain Trust."](#)

20.9 Overriding the Default Security Settings

By default, all access to Personalization REST resources (other than the resourceIndex) requires authentication. In most cases this will be sufficient for development. However, for production environments, you may want to modify the default security constraints. The following sections describe how to set up less security to execute scenarios (where anonymous access is needed), and more security to prevent the ability to create new scenarios.

This section contains the following subsections:

- [Section 20.9.1, "Allowing Anonymous Execution of Scenarios"](#)
- [Section 20.9.2, "Disabling Scenario Creation by Anonymous Users"](#)
- [Section 20.9.3, "Disabling Scenario Creation by Authenticated Users"](#)

20.9.1 Allowing Anonymous Execution of Scenarios

Adding the following security constraint to the domain's `conductor-extensions-library\WEB-INF\web.xml` file will honor default descriptor (authentication required) security, plus allow anonymous GET/POST on scenarios created or deployed from an anonymous application or namespace:

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>ConductorJerseyWebApplication</web-resource-name>
    <url-pattern>/api/conductor/namespaces/anonymous/scenarios/*</url-pattern>
    <http-method>GET</http-method>
    <http-method>POST</http-method>
  </web-resource-collection>
  <!-- Allow anonymous user access in this namespace -->
  <!--auth-constraint>
    <role-name>Users</role-name>
  </auth-constraint-->
</security-constraint>
```

20.9.2 Disabling Scenario Creation by Anonymous Users

You can disable scenario creation for any anonymous user using a simple filter that you add to the domain's `conductor-extensions-library\WEB-INF\web.xml` file. An example filter (`AnonymousScenarioFilter`) is shown below:

```
<filter>
  <filter-name>AnonymousScenarioFilter</filter-name>
  <filter-class>oracle.wcps.samples.AnonymousScenarioFilter</filter-class>
</filter>
<filter-mapping>
  <filter-name>AnonymousScenarioFilter</filter-name>

  <url-pattern>/api/conductor/namespaces/PublicPersonalization/scenarios/</url-pattern>
</filter-mapping>
<security-constraint>
  <web-resource-collection>
    <web-resource-name>ConductorJerseyWebApplication</web-resource-name>

    <url-pattern>/api/conductor/namespaces/PublicPersonalization/scenarios/*</url-pattern>

    <http-method>GET</http-method>
    <http-method>POST</http-method>
```

```
</web-resource-collection>
<!--
  Commented out to allow anonymous user access in this namespace
<auth-constraint>
<role-name>Users</role-name>
</auth-constraint>
-->
</security-constraint>
```

The filter explicitly checks for an anonymous user (`httpRequest.getUserPrincipal() == null`) and an HTTP POST operation on the `/api/conductor/namespaces/PublicPersonalization/scenarios` URL, which is the REST resource for creating a scenario.

```
public void doFilter(ServletRequest request, ServletResponse response, FilterChain
chain)
    throws IOException, ServletException
{
    if (request instanceof HttpServletRequest)
    {
        HttpServletRequest httpRequest = (HttpServletRequest)request;
        String method = httpRequest.getMethod();
        if ("POST".equalsIgnoreCase(method) && httpRequest.getUserPrincipal()
== null)
        {
            throw new ServletException("Anonymous users cannot create
scenarios.");
        }
    }
    chain.doFilter(request, response);
}
```

20.9.3 Disabling Scenario Creation by Authenticated Users

A simple change to the filter described in [Section 20.9.2, "Disabling Scenario Creation by Anonymous Users"](#) (removing the `httpRequest.getUserPrincipal()` check) would disable scenario creation for all users. Although the HTTP POST operation is also used to request execution of scenarios, the URI in that case is different (and protected in the `<security-constraint>` not the filter `<url-pattern>`).

Managing the RSS Service

This chapter describes how to configure and manage the RSS service for the Spaces application and Framework applications.

This chapter includes the following sections:

- [Section 21.1, "What You Should Know About the RSS Service"](#)
- [Section 21.2, "RSS Prerequisites"](#)
- [Section 21.3, "Setting Up a Proxy Server for External RSS News Feeds"](#)
- [Section 21.4, "Testing External RSS News Feed 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."](#)

21.1 What You Should Know About the RSS Service

The RSS service encompasses the RSS Viewer and the service to show news feeds from various WebCenter Portal services. The RSS Viewer enables users to view external news feeds from different web sites from within WebCenter Portal applications. The RSS service delivers content update information from the following WebCenter Portal services: Recent Activities, Discussions, Lists, and Announcements.

21.2 RSS Prerequisites

The RSS service does not require any back-end server. You do not need to set up a connection to use this service. However, depending on your network configuration, you may need to set up a proxy server to enable your WebCenter Portal applications to display content from external RSS news feeds.

21.3 Setting Up a Proxy Server for External RSS News Feeds

To enable external RSS news feeds in your WebCenter Portal applications, you must set up a proxy server.

A proxy server is also required if you want to display external links in Activity Stream task flows. Both the RSS service and the Activity Stream service share the same proxy server settings.

You can configure a proxy server by using either Fusion Middleware Control or WLST. For information, see [Section 9.7, "Setting Up a Proxy Server."](#)

21.4 Testing External RSS News Feed Connections

After setting up the proxy server for the RSS Viewer of the RSS service, you can test the connection to make sure you can access external RSS feeds.

To ensure the proxy server is accurately configured for the RSS Viewer:

1. In your WebCenter Portal application, add the RSS task flow to a page.
2. Edit the RSS task flow and set the URL to an external RSS feed. For example:

```
http://www.oracle.com/rss/rss_ocom_pr.xml
```

If the RSS feed renders correctly, it confirms that the proxy configuration is set up properly.

For information about adding the RSS task flow and editing the URL, see the "Working with the RSS Service" chapter in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

Managing Oracle SES Search in WebCenter Portal

This chapter describes how to configure the Oracle Secure Enterprise Search (SES) adapter to index and search most WebCenter Portal objects. Oracle SES search is beneficial for the following reasons:

- Oracle SES search provides unified ranking results, with the most relevant items appearing first.
- Oracle SES search allows search of other repositories outside of WebCenter Portal.
- Oracle SES search supports the Search service REST APIs and data control for customizing your search interface.

With **WebCenter Portal: Framework applications**, Oracle SES is set as the default and preferred search platform. Detailed configuration steps are in [Section 22.5, "Configuring Oracle SES to Search Framework Applications."](#)

With **WebCenter Portal: Spaces applications**, WebCenter Portal's internal Search service adapters are set as the default search platform; however, large-scale implementations should be configured to use Oracle SES for best performance. Detailed configuration steps are in [Section 22.6, "Configuring Oracle SES to Search Spaces Applications."](#)

The information in this chapter is *not* required if you choose to use WebCenter Portal's original Search service adapters.

Always use Fusion Middleware Control or the WLST command-line tool to review and configure back-end services for WebCenter Portal applications. Any changes that you make to applications, post deployment, are stored in MDS metadata store as customizations. See [Section 1.3.5, "WebCenter Portal Configuration Considerations."](#)

Note: Most changes that you make to Search configuration, through Fusion Middleware Control or using WLST, are not dynamic. You must restart the managed server on which the WebCenter Portal application is deployed (by default, WC_Spaces) for your changes to take effect. See [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

This chapter includes the following sections:

- [Section 22.1, "What You Should Know About WebCenter Portal's Search with Oracle SES"](#)
- [Section 22.2, "Configuration Roadmaps for Oracle SES in WebCenter Portal"](#)

- [Section 22.3, "Prerequisites for using Oracle SES"](#)
- [Section 22.4, "Setting Up Oracle SES Connections"](#)
- [Section 22.5, "Configuring Oracle SES to Search Framework Applications"](#)
- [Section 22.6, "Configuring Oracle SES to Search Spaces Applications"](#)
- [Section 22.7, "Troubleshooting Issues with Oracle SES Search"](#)

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."](#)

22.1 What You Should Know About WebCenter Portal's Search with Oracle SES

Oracle recommends Oracle SES search for best performance. You can configure Oracle SES to search WebCenter Portal applications for the following resources:

- Documents, including wikis and blogs
- Announcements and Discussions
- Spaces, lists, page content, and people resources in WebCenter Portal: Spaces

Note: WebCenter Portal: Spaces includes the additional Oracle SES crawler that indexes spaces, lists, pages, and people resources in Spaces. This crawler is not supported in Framework applications.

Results from all sources are listed together, with the most relevant items appearing first. For example, when you run a search for a user name, most likely, you are looking for that person's contact information (that is, the exact user name in the People Connections service), not necessarily documents that the user wrote. The unified ranking results in Oracle SES allow you to see the most relevant results, across all different types of searches, without configuring Search Preferences.

When Oracle SES is configured to search WebCenter Portal, other non-crawled resources (for example, notes and events) are not returned in search results.

Three types of Oracle SES crawlers index WebCenter Portal resources:

- **Documents Crawler:** (For both Framework and Spaces applications.) This uses the Oracle SES Oracle Content Server source type to crawl documents, including wikis and blogs.
- **Discussions Crawler:** (For both Framework and Spaces applications.) This uses the Oracle SES Database source type to crawl discussions and announcements.
- **Spaces Crawler:** (For Spaces applications only.) This uses the Oracle SES Oracle WebCenter source type to crawl certain objects in Spaces, such as lists, pages, spaces, and people connections profiles.

Note: Oracle SES crawls information collected as a *source*. Each source has a *type* that identifies where the information is stored, such as in a database or a content repository.

When you configure Oracle SES to search WebCenter Portal, all available Oracle SES crawlers should be enabled. It is not recommended to enable one of these Oracle SES crawlers and not another. For example, when you configure Oracle SES to search Framework applications, you cannot have it crawl documents and not discussions.

22.2 Configuration Roadmaps for Oracle SES in WebCenter Portal

Use the roadmaps in this section as an administrator's guide through the configuration process:

- **Roadmap - Configuring Oracle SES for Framework Applications**

[Figure 22-1](#) and [Table 22-1](#) provide an overview of the prerequisites and tasks required to get Oracle SES working in Framework applications.

Figure 22-1 Configuring Oracle SES for Framework Applications

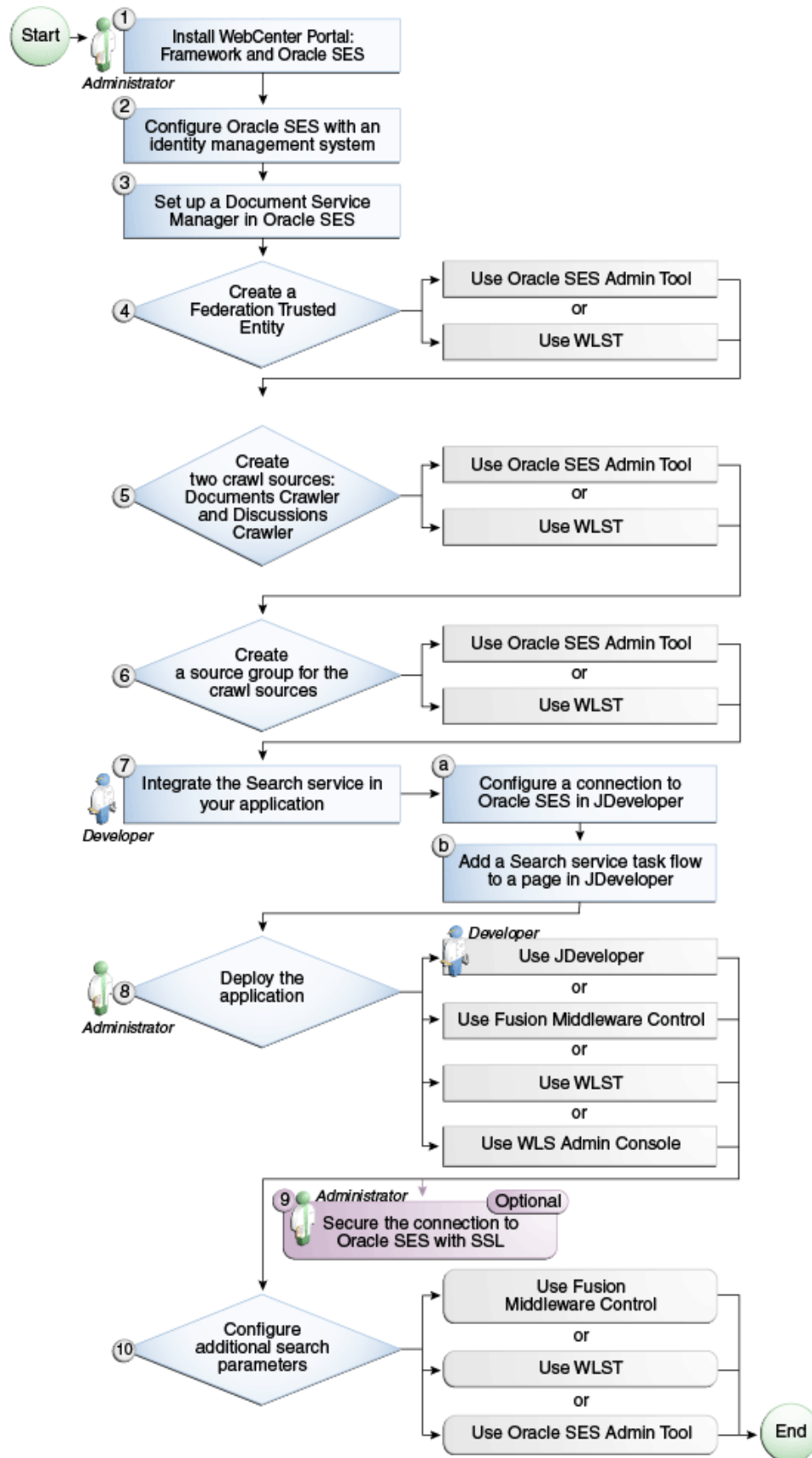


Table 22–1 Configuring Oracle SES for Framework Applications

Actor	Task	Sub-task
Administrator	1. Install WebCenter Portal and Oracle SES	
	2. Configure Oracle SES with an identity management system	
	3. Set up a Document Service Manager in Oracle SES	
	4. Create a Federation Trusted Entity using one of the following tools:	
	<ul style="list-style-type: none"> ■ Oracle SES Admin Tool ■ WLST 	
	5. Create two crawl sources: Documents Crawler and Discussions Crawler using one of the following tools:	
<ul style="list-style-type: none"> ■ Oracle SES Admin Tool ■ WLST 		
Developer	7. Integrate the Search service in your Framework application	7.a Configure a connection to Oracle SES in JDeveloper
		7.b Add a Search service task flow to a page in JDeveloper
Developer or Administrator	8. Deploy the Framework application using one of the following tools:	
	<ul style="list-style-type: none"> ■ JDeveloper (Developer) ■ Fusion Middleware Control (Administrator) ■ WLST (Administrator) ■ WLS Admin Console (Administrator) 	
Administrator	9. (Optional) Secure the connection to Oracle SES with SSL	
Administrator	10. Configure additional search parameters using one of the following tools:	
		<ul style="list-style-type: none"> ■ Fusion Middleware Control ■ WLST ■ WLS Admin Console

- **Roadmap - Configuring Oracle SES for Spaces Applications**

[Figure 22–2](#) and [Table 22–2](#) provide an overview of the prerequisites and tasks required to get Oracle SES working in Spaces.

Figure 22–2 Configuring Oracle SES for Spaces Applications

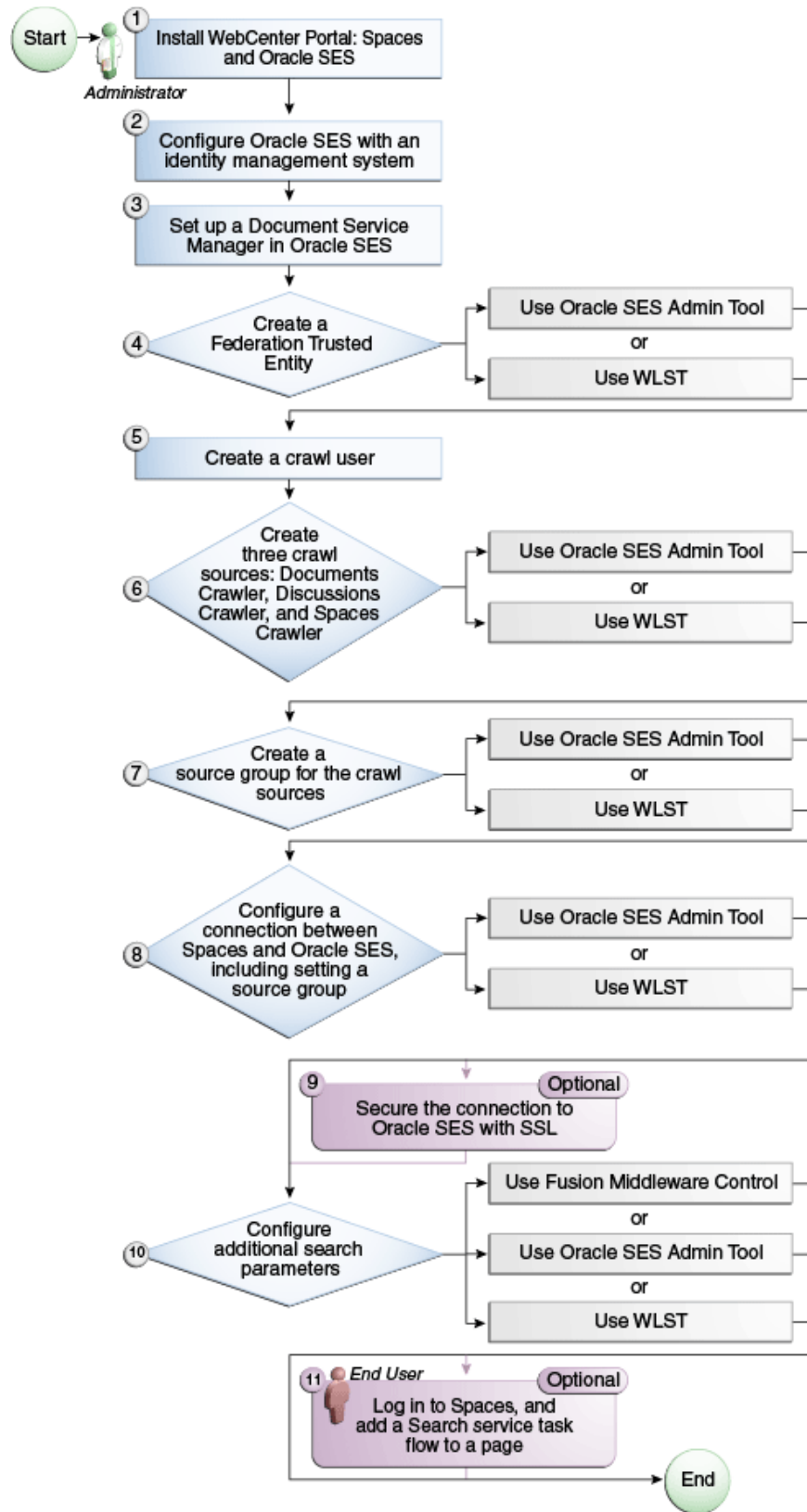


Table 22–2 Configuring Oracle SES for Spaces Applications

Actor	Task
Administrator	1. Install WebCenter Portal and Oracle SES
	2. Configure Oracle SES with an identity management system
	3. Set up a Document Service Manager in Oracle SES
	4. Create a Federation Trusted Entity using one of the following tools: <ul style="list-style-type: none"> ■ Oracle SES Admin Tool ■ WLST
	5. Create a crawl user
	6. Create three crawl sources: Documents Crawler, Discussions Crawler, and Spaces Crawler using one of the following tools: <ul style="list-style-type: none"> ■ Oracle SES Admin Tool ■ WLST
	7. Create a source group for the crawl sources using one of the following tools: <ul style="list-style-type: none"> ■ Oracle SES Admin Tool ■ WLST
	8. Configure a connection between Spaces and Oracle SES using one of the following tools: <ul style="list-style-type: none"> ■ Oracle SES Admin Tool ■ WLST
	9. (Optional) Secure the connection to Oracle SES with SSL
	10. Configure additional search parameters using one of the following tools: <ul style="list-style-type: none"> ■ Fusion Middleware Control ■ Oracle SES Admin Tool ■ WLST
End User	11. (Optional) Add a Search service task flow to a space in Spaces

22.3 Prerequisites for using Oracle SES

This section includes the following subsections:

- [Section 22.3.1, "Oracle SES - Installation"](#)
- [Section 22.3.2, "Oracle SES - Configuration"](#)
- [Section 22.3.3, "Oracle SES - Security"](#)

22.3.1 Oracle SES - Installation

Supported Oracle SES versions include 10.1.8.4.x and later. Oracle strongly recommends using Oracle SES release 11.1.2.2. For Oracle SES installation directions, see the section, "Back-End Requirements for the Search Service" in *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Portal*.

See Also: It is important to verify that you have installed all required patches for Oracle SES. For the latest information on required patches, check the Release Notes.

This chapter assumes that you are running the latest supported products: Oracle SES 11.1.2.2 and Oracle WebCenter Content: Content Server 11.1.1.5; however, the following scenarios also are supported.

WebCenter Portal: Framework versions 11.1.1.3 and 11.1.1.4 are supported with these installations:

- Oracle SES 11.1.2 with Oracle Content Server 11.1.1.3+
- Oracle SES 10.1.8.4 with Oracle Content Server 11.1.1.3+
- Oracle SES 10.1.8.4 with Oracle Content Server 10.1.3.5.1 (version included from 11.1.1.1 to 11.1.1.3)

WebCenter Portal: Spaces versions 11.1.1.3 and 11.1.1.4 are supported with these installations:

- Oracle SES 11.1.2 with Oracle Content Server 11.1.1.3+
- Oracle SES 10.1.8.4 with Oracle Content Server 11.1.1.3

22.3.2 Oracle SES - Configuration

1. Oracle SES must be configured with an identity management system to validate and authenticate users. This is necessary for secure searches, so searches return only results that the user is allowed to view based on access privileges.

Because WebCenter Portal uses identity propagation when communicating with Oracle SES, WebCenter Portal's user base must match that in Oracle SES. One way this can happen is by configuring WebCenter Portal and Oracle SES to the same identity management system, such as Oracle Internet Directory.

Note: For information on all supported identity management systems, see [Section 28.2.3, "Default Identity and Policy Stores."](#)

Only one identity plug-in can be set up for each Oracle SES instance. All repositories (Oracle WebCenter Content: Content Server, Oracle WebCenter Portal Discussions Server, and Oracle WebCenter Portal: Spaces) must share the same user base as Oracle SES.

Oracle SES includes numerous identity plug-ins for identity management systems including Oracle Internet Directory, Oracle Content Server, and Microsoft Active Directory. For information, see the Oracle SES documentation included with the product. (This is listed in the WebCenter Portal product area on the Oracle Fusion Middleware documentation library.)

The following example sets up the identity plug-in for Oracle Internet Directory:

- a. In the Oracle SES administration tool, navigate to the Global Settings - Identity Management Setup page, select **Oracle Internet Directory** from the available identity plug-ins, and click **Activate**.

- b. Provide the following values:

Host name: The host name of the computer where Oracle Internet Directory is running

Port: The Oracle Internet Directory port number

Use SSL: `true` or `false`, based on your preference

Realm: The Oracle Internet Directory realm, for example,
dc=us, dc=oracle, dc=com

User name: The Oracle Internet Directory admin user name; for example,
cn=orcladmin

Password: Admin user password

- c. Click **Submit**.
2. Each Oracle SES instance must have a trusted entity for allowing WebCenter Portal end users to be securely propagated at search time. (A trusted entity allows the WebCenter Portal application to authenticate itself to Oracle SES and assert its users when making queries on Oracle SES.) This trusted entity can be any user that either exists on the identity management server behind Oracle SES or is created internally in Oracle SES.

You can do this either in WLST or in Oracle SES.

Note: This trusted entity name and password is required later as the `appUser` and `appPassword` properties in the WLST command `createSESConnection`.

To do this with WLST, use the `createFederationTrustedEntity` command (Example 22-1).

Example 22-1 createFederationTrustedEntity Command

```
createFederationTrustedEntity(
'webcenter', 'http://ses-host:ses-port/search/api/admin/AdminService',
'ses-admin-pw', 'webcenter-proxy-user', 'webcenter-proxy-user-pw',
'Trusted entity for WebCenter');
```

where:

- `ses-host` = Oracle SES host name
- `ses-port` = Oracle SES port number
- `ses-admin-pw` = Oracle SES admin user password
- `webcenter-proxy-user` = Proxy user to log on WebCenter Portal end users
- `webcenter-proxy-user-pw` = Password of proxy user to log on WebCenter Portal end users

For command syntax and examples, see the section, "createFederationTrustedEntity" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

To do this in Oracle SES, follow these steps.

- a. In the Oracle SES administration tool, navigate to the Global Settings - Federation Trusted Entities page.
- b. Enter a name for a trusted entity. This is the name that WebCenter Portal uses to authenticate itself to Oracle SES at search time (before it propagates the end user identity to Oracle SES).

To allow the entity to be authenticated through the active identity plug-in:

- Make sure that the entity name is the name of a user that exists in the identity management system.

- Leave the password field blank.
- Select the **Use Identity Plug-in for authentication** checkbox.
- Enter the authentication attribute value corresponding to the Authentication Attribute in your active identity plug-in.

To allow the entity to be authenticated through Oracle SES:

- Enter any user name (for example, `wcsearch`) and password (for example, `welcome1`).
- Do *not* select the **Use Identity Plug-in for authentication** checkbox.

For more information, see the online help for the Federation Trusted Entities page in Oracle SES.

Note: For reference, the following sample user names are used in this chapter:

- `wcsearch`: User of the Oracle SES Federation Trusted Entity
 - `mycrawladmin`: Crawl admin user in Spaces and in the identity management system to crawl certain Spaces objects, such as lists, pages, spaces, and people connections profiles
 - `sescrawler` (or admin user): Crawl admin user in Oracle WebCenter Content Server with `sescrawlerrole` (or admin) role
-

22.3.3 Oracle SES - Security

Most enterprise deployments require that their HTTP connections be secure. SSL (secure socket layer) is an encryption protocol for securely transmitting private content on the internet. Oracle strongly recommends that you use an SSL-protected channel to transmit password and other secure data over networks.

For instructions, see [Section 33.10, "Securing the Connection to Oracle SES with SSL."](#)

22.4 Setting Up Oracle SES Connections

This section includes the following subsections:

- [Section 22.4.1, "Registering Oracle Secure Enterprise Search Servers"](#)
- [Section 22.4.2, "Choosing the Active Oracle SES Connection"](#)
- [Section 22.4.3, "Modifying Oracle SES Connection Details"](#)
- [Section 22.4.4, "Deleting Oracle SES Connections"](#)
- [Section 22.4.5, "Testing Oracle SES Connections"](#)

22.4.1 Registering Oracle Secure Enterprise Search Servers

You can register multiple Oracle SES connections with a WebCenter Portal application but only one of them is active at a time.

You can register Oracle SES connections using either Fusion Middleware Control or WLST. This section includes the following subsections:

- [Section 22.4.1.1, "Registering Oracle SES Search Connections Using Fusion Middleware Control"](#)

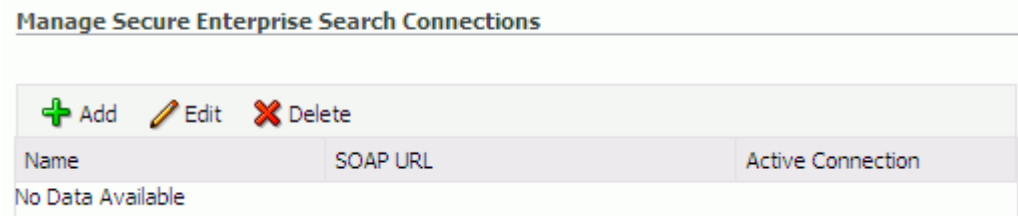
- [Section 22.4.1.2, "Registering Oracle SES Connections Using WLST"](#)

22.4.1.1 Registering Oracle SES Search Connections Using Fusion Middleware Control

To register an Oracle SES instance with WebCenter Portal applications:

1. Log in to Fusion Middleware Control and navigate to the home page for the WebCenter Portal application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
3. From the list of services on the WebCenter Portal Service Configuration page, select **Search**.
4. To connect to a new Oracle SES instance, click **Add** ([Figure 22-3](#)).

Figure 22-3 Configuring Oracle Secure Search Services



5. On the Add Secure Enterprise Search Connection page, enter a unique name for this connection, and indicate whether this connection is the active (or default) connection for the application ([Figure 22-4](#)).

Figure 22-4 Add Secure Enterprise Search Connection

[Table 22-3](#) describes the connection parameters.

Table 22–3 Search Connection - Name

Field	Description
Connection Name	Enter a unique name for the connection. The name must be unique (across all connection types) within the WebCenter Portal application.
Active Connection	Select to use the Oracle SES instance defined on this connection to search repositories outside the WebCenter Portal application and include Oracle SES search results in your result set. While you can register multiple search connections for an application, only one connection is used by the Search service—the default (or active) connection.

6. Enter connection details for the Oracle SES instance ([Table 22–4](#)).

Table 22–4 Oracle Secure Enterprise Search - Connection Details

Field	Description
SOAP URL	Enter the Web Services URL that Oracle SES exposes to enable search requests. Use the format: <code>http://host:port/search/query/OracleSearch</code> For example: <code>http://myHost:7777/search/query/OracleSearch</code>
Federation Trusted Entity Name	Enter the user name of the Oracle SES Federation Trusted Entity created in Section 22.3.2, "Oracle SES - Configuration." Tip: This user is configured in the Oracle SES administration tool, on the Global Settings - Federation Trusted Entities page. The WebCenter Portal application must authenticate itself as a trusted application to Oracle SES to perform searches on behalf of WebCenter Portal users. Examples in this chapter use <code>wcsearch</code> for this value.
Federation Trusted Entity Password	Enter the password for the Federation Trusted Entity.

7. Click **OK** to save this connection.

Note: To start using the new (active) connection you must restart the managed server on which the application is deployed. For more information, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

22.4.1.2 Registering Oracle SES Connections Using WLST

1. Use the WLST command `createSESConnection` to create a connection to Oracle SES. For example:

```
createSESConnection(appName='webcenter',
                   name='MySesConnection',
                   url='http://myhost.com:7777/search/query/OracleSearch',
                   appUser='wcsearch',
                   appPassword='welcome1',
                   default=true)
```

where `appUser` is the user name of the Oracle SES Federation Trusted Entity created in [Section 22.3.2, "Oracle SES - Configuration."](#)

For command syntax and examples, see the section, "createSESConnection" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

To configure the Search service to actively use a new Oracle SES connection, set `default=true`. For more information, see [Section 22.4.2.2, "Choosing the Active Oracle SES Connection Using WLST."](#)

See Also: [Section 22.4.3.2, "Modifying Oracle SES Connection Details Using WLST"](#)

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

Note: To start using the new (active) connection or settings, you must restart the managed server on which the application is deployed (by default, `WC_Spaces`). See "Starting and Stopping WebLogic Managed Servers Using the Command Line" in *Oracle Fusion Middleware Administrator's Guide*.

22.4.2 Choosing the Active Oracle SES Connection

You can register multiple Oracle SES connections with a WebCenter Portal application but only one connection is active at a time.

Note: These steps in this section are not necessary if you selected the active connection in [Section 22.4.1, "Registering Oracle Secure Enterprise Search Servers."](#)

This section includes the following subsections:

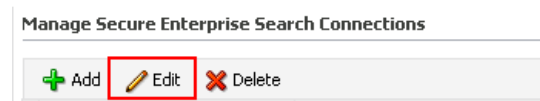
- [Section 22.4.2.1, "Choosing the Active Oracle SES Connection Using Fusion Middleware Control"](#)
- [Section 22.4.2.2, "Choosing the Active Oracle SES Connection Using WLST"](#)

22.4.2.1 Choosing the Active Oracle SES Connection Using Fusion Middleware Control

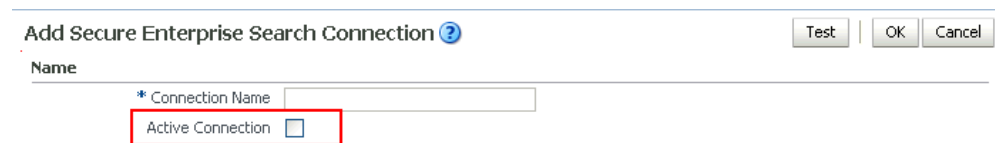
To change the active connection:

1. Log in to Fusion Middleware Control and navigate to the home page for the WebCenter Portal application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.

- From the list of services on the WebCenter Portal Services Configuration page, select **Search**.
The Manage Secure Enterprise Search Connections table indicates the current active connection (if any).
- Select the connection you want to make the active (or default) connection, and then click **Edit** (Figure 22–5).

Figure 22–5 Edit Icon

- Select the **Active Connection** checkbox (Figure 22–6).

Figure 22–6 Active Connection Checkbox

- Click **OK** to update the connection.

Note: To start using the new (active) connection you must restart the managed server on which the application is deployed. For more information, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

22.4.2.2 Choosing the Active Oracle 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 the section, "setSESConnection" in *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 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

Note: To start using the active connection you must restart the managed server on which the application is deployed (by default, WC_Spaces). For more information, see the section, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in *Oracle Fusion Middleware Administrator's Guide*.

22.4.3 Modifying Oracle 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 Portal application is deployed.

Note: The steps in this section are required only to modify the details configured in [Section 22.4.1, "Registering Oracle Secure Enterprise Search Servers."](#)

This section includes the following subsections:

- [Section 22.4.3.1, "Modifying Oracle SES Connection Details Using Fusion Middleware Control"](#)
- [Section 22.4.3.2, "Modifying Oracle SES Connection Details Using WLST"](#)

22.4.3.1 Modifying Oracle SES Connection Details Using Fusion Middleware Control

To update connection details for an Oracle SES instance:

1. Log in to Fusion Middleware Control and navigate to the home page for the WebCenter Portal application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
3. From the list of services on the WebCenter Portal Service Configuration page, select **Search**.
4. Select the connection name, and click **Edit**.
5. Edit connection details, as required. For detailed parameter information, see [Table 22-4](#).
6. Click **OK** to save your changes.

Note: To start using the updated (active) connection you must restart the managed server on which the application is deployed. For more information, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

22.4.3.2 Modifying Oracle SES Connection Details Using WLST

Use the WLST command `setSESConnection` to alter an existing Oracle SES search connection. For command syntax and examples, see the section, "setSESConnection" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

Note: To start using the updated (active) connection you must restart the managed server on which the application is deployed (by default, WC_Spaces). For more information, see the section "Starting and Stopping WebLogic Managed Servers Using the Command Line" in *Oracle Fusion Middleware Administrator's Guide*.

22.4.4 Deleting Oracle 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 are not able to search content on external repositories.

This section includes the following subsections:

- [Section 22.4.4.1, "Deleting Search Connections Using Fusion Middleware Control"](#)
- [Section 22.4.4.2, "Deleting Search Connections Using WLST"](#)

22.4.4.1 Deleting Search Connections Using Fusion Middleware Control

To delete an Oracle SES server connection:

1. Log in to Fusion Middleware Control and navigate to the home page for the WebCenter Portal application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
3. From the Service Connection drop-down, select **Search**.
4. Select the connection name, and click **Delete**.

Figure 22–7 Delete Connection Icon



Note: To effect this change you must restart the managed server on which the application is deployed. For more information, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

22.4.4.2 Deleting Search Connections Using WLST

Use the WLST command `deleteConnection` to remove a search connection. For command syntax and examples, see the section, "deleteConnection" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

Note: To effect this change you must restart the managed server on which the application is deployed (by default, WC_Spaces). For more information, see the section "Starting and Stopping WebLogic Managed Servers Using the Command Line" in *Oracle Fusion Middleware Administrator's Guide*.

22.4.5 Testing Oracle SES Connections

Confirm the Oracle SES connection by entering in a browser the URL for Oracle SES Web Services operations:

```
http://host:port/search/query/
```

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.

22.5 Configuring Oracle SES to Search Framework Applications

With WebCenter Portal: Framework applications, Oracle SES is set as the default and preferred search platform. Configuring Oracle SES to search Framework applications requires similar steps to configuring Oracle SES to search Spaces applications, but Framework applications do not support the Spaces Crawler.

Note: For an overview of the tasks that must be performed to enable Oracle SES as the search engine in Framework applications, see [Section 22.2, "Configuration Roadmaps for Oracle SES in WebCenter Portal."](#) There may be various acceptable ways and orders to perform the required tasks.

This section describes the steps to set up Oracle SES to search Framework applications:

- [Section 22.5.1, "Setting Up Oracle WebCenter Portal Content Server for Oracle SES Search"](#)
- [Section 22.5.2, "Setting Up Oracle WebCenter Portal's Discussion Server for Oracle SES Search"](#)
- [Section 22.5.3, "Setting Up Oracle SES to Search WebCenter Portal"](#)
- [Section 22.5.4, "Setting Up WebCenter Portal: Framework for Oracle SES Search"](#)
- [Section 22.6.7, "Tips for Crawling Page Contents"](#)

See Also: [Section 22.1, "What You Should Know About WebCenter Portal's Search with Oracle SES"](#)

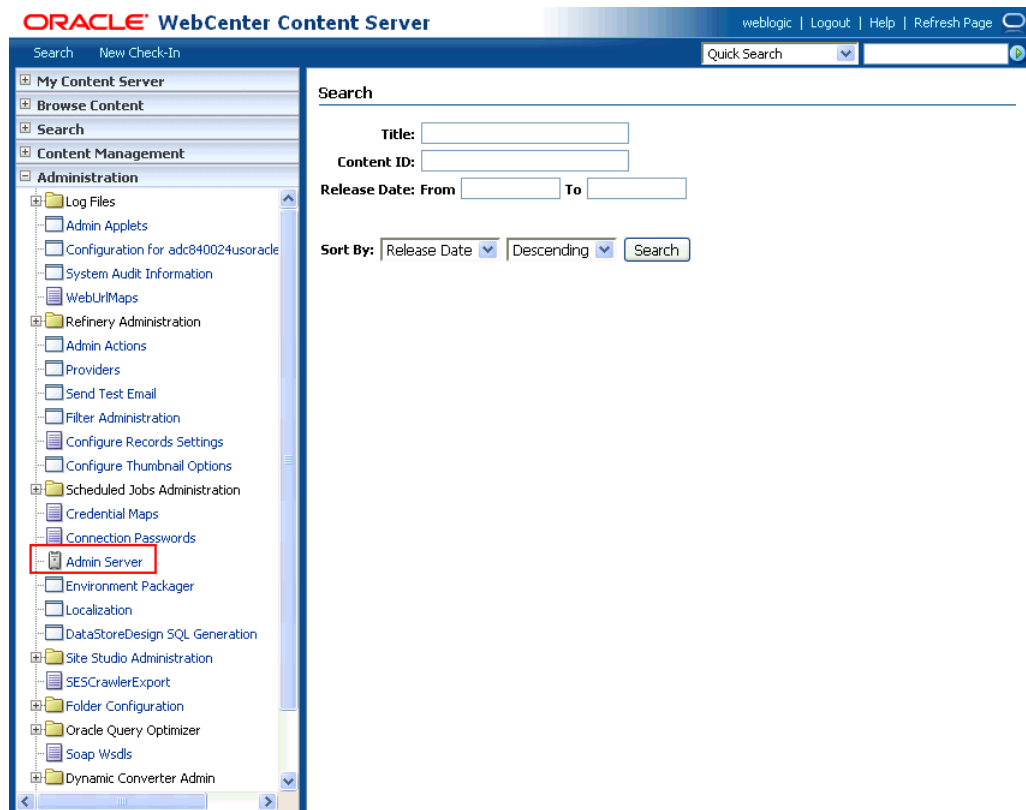
22.5.1 Setting Up Oracle WebCenter Portal Content Server for Oracle SES Search

This section describes how to configure Oracle WebCenter Content: Content Server to be crawlable by Oracle SES (in particular, the Content Server that WebCenter Portal uses for storing documents).

The following steps must be done from within the Content Server.

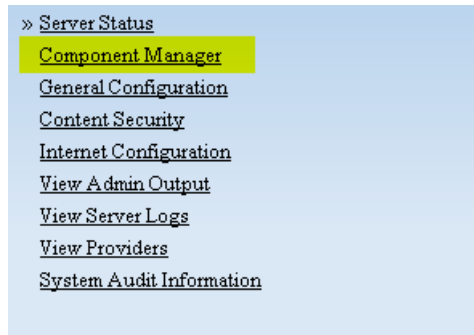
1. Create the role `sescrawlerrole`.
2. Create the user `sescrawler`, and assign it the `admin` role and the `sescrawlerrole` role. This user creates the Content Server source in Oracle SES.
3. Add `sceCrawlerRole=sescrawlerrole` to `config.cfg`.
4. Restart the Content Server.
5. In the Content Server console, install the `SESCrawlerExport` component on the content server, if not done:
 - a. Log on to the Content Server as a system administrator. For example:
`http://host:port/cs.`
 - b. From the Administration dropdown menu, select **Admin Server** (Figure 22–8).

Figure 22–8 Content Server Administration



- c. Click the button with the instance name.
- d. Click **Component Manager** from the menu list on the left pane (Figure 22–9).

Figure 22–9 Content Server Component Manager



- e. Select **SESCrawlerExport** under Integration and click **Update**.
- f. Enter configuration parameters. (You can change configuration parameters after installation.)

Disable security on authentication and authorization APIs provided by the SESCrawlerExport; that is, set **Disable Secure APIs** to `false`. This lets security provided by the SESCrawlerExport be done internally instead of by the Content Server.

Additionally, in clustered environments only, the **feedLoc** parameter must specify a location on the shared disk accessed by the nodes of content server, and they each must reference it the same way; for example, `sharedDrive/dir1/dir2`. Note that this is not the default location (relative path) provided.

- g. Restart the Content Server.
6. Take a snapshot of the Content Server repository.
- a. Log on to the Content Server as a system administrator. For example: `http://host:port/cs`.
 - b. From the Administration dropdown menu, select **SESCrawlerExport**.
 - c. Select **All sources**, and click **Take Snapshot** (Figure 22–10).

Figure 22–10 Content Server Snapshot



It is important to take a snapshot before the first crawl or any subsequent full crawl of the source.

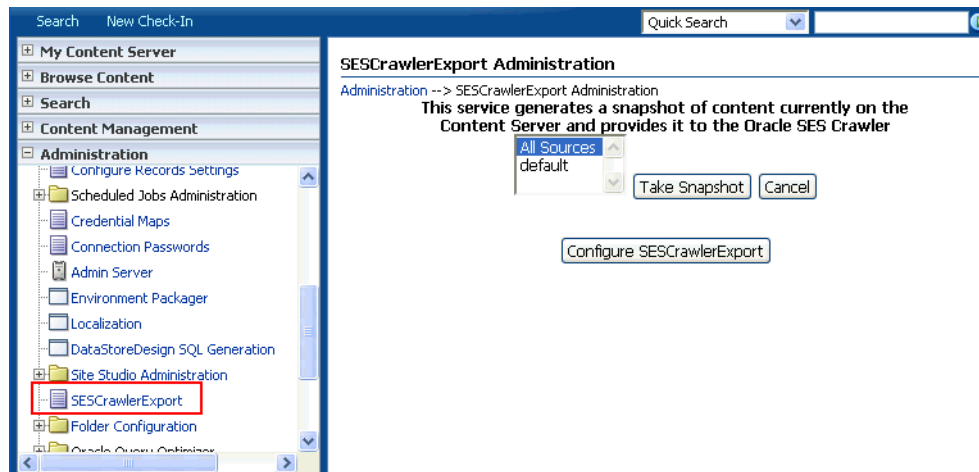
The snapshot generates `configFile.xml` at the location specified during component installation, and feeds are created at the subdirectory with the source name under **feedLoc**.

7. If the Content Server is configured for web rendition, then items in the Content Server are rendered in PDF format. The content item's native MIME type rendition is overwritten. For example, the MIME type of a Microsoft Office Word document is 'application/msword', but when the Content Server uses web rendition the MIME type becomes 'application/pdf'. A search query with the `Mimetype` parameter set to 'application/msword' does not return Word documents.

If your Content Server is configured to use web rendition, then you must configure the Content Server metadata list to include the `dFormat` value, so that required MIME types are exported to Oracle SES. This is necessary to be able to narrow searches by MIME type.

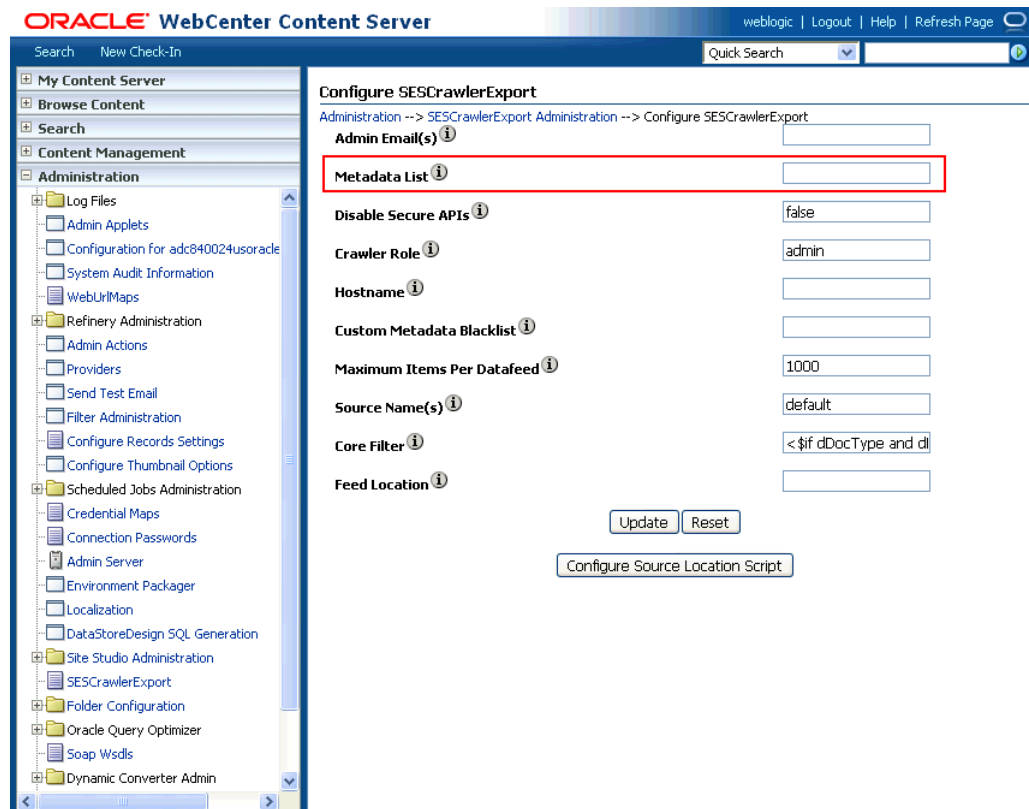
- a. Back on the `SESCrawlerExport` Administration page, click **Configure SESCrawlerExport** (Figure 22–11).

Figure 22–11 Content Server Snapshot



- b. By default, the **Metadata List** field is blank (Figure 22–12).

Figure 22–12 Content Server Metadata List



Left blank, the list of metadata values that are exported to Oracle SES consists of the following (plus any custom metadata fields beginning with 'x'):

dID, dDocName, dRevLabel, dDocType, dDocAccount, dSecurityGroup, dOriginalName, dReleaseDate, dOutDate.

However, the dFormat value must be added to this list.

When the blank default value is changed, the default values are removed, so they also must be added back. To include dFormat with the standard attributes, enter the following value for **Metadata List**:

dFormat, dID, dDocName, dRevLabel, dDocType, dDocAccount, dSecurityGroup, dOriginalName, dReleaseDate, dOutDate

- c. Optionally, add to this list any custom metadata values you require (beginning with x).

For example, the following entry for **Metadata List** includes custom attributes:

dFormat, dID, dDocName, dDocType, dDocAccount, dSecurityGroup, dOriginalName, dReleaseDate, dDocAuthor, dDocCreator, dDocCreatedDate, dOutDate, xCollectionID, xWCTags, xComments, xRegionDefinition

See Also:

- For information about displaying MIME types in search results, see "Customizing Search Results with Attributes and Refiners" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*
- For detailed information on Content Server configuration, see the `Deployment Guide.pdf` included with the product.

22.5.2 Setting Up Oracle WebCenter Portal's Discussion Server for Oracle SES Search

This section describes how to configure Oracle WebCenter Portal's Discussion Server to be crawlable by Oracle SES (in particular, the discussions server that WebCenter Portal uses for storing discussions and announcements).

Note: These steps is not required if you have a new installation of WebCenter Portal (with an Oracle database) and Oracle WebCenter Portal's Discussion Server. It is only required if you are using upgraded (patched) instances.

You can find database schema details for the corresponding data sources from your Oracle WebLogic Server console.

1. Run the Repository Creation Utility (RCU) to confirm that the Discussions Crawler WebCenter Portal component has been installed on the system.
 - Oracle databases:

Verify that the Oracle WebCenter Portal's Discussion Server back end has been configured properly by noting that the *MyPrefix_DISCUSSIONS* user is installed in RCU.

Then verify that the Discussions Crawler has been configured properly by noting that the *MyPrefix_DISCUSSIONS_CRAWLER* user is installed in RCU.
 - Microsoft SQL Server databases:

Verify that the Oracle WebCenter Portal's Discussion Server back end has been configured properly by noting that the *MyPrefix_DISCUSSIONS* user is installed in RCU.

Then verify that the Discussions Crawler has been configured properly by noting that the *MyPrefix_DISCUSSIONS_CRAWLER* user is installed in RCU.
 - IBM DB2 databases:

Verify that the Oracle WebCenter Portal's Discussion Server back end has been configured properly by noting that the *MyPrefix_DS* user is installed in RCU.

Then verify that the Discussions Crawler has been configured properly by noting that the *MyPrefix_DC* user is installed in RCU.

Note: For IBM DB2 databases, *MyPrefix* is limited to five characters. IBM DB2 uses operating system users for authentication (that is, the database user is actually an operating system user). Because some operating systems have an eight character limit for user names, this requires an eight character user name.

If the Discussions Crawler component is not installed, then you must install it using RCU, selecting the same prefix that was used for the Oracle WebCenter Portal's Discussion Server component. Also, during the tablespace specification step in RCU, select *Prefix_IAS_DISCUSSIONS* as the default tablespace. This installs the user for Oracle SES.

For more information, see [Chapter 7, "Deploying WebCenter Portal: Framework Applications."](#)

2. Run the following tool to upgrade the data in the Oracle WebCenter Portal's Discussion Server database schema, if you have not run the tool yet:

```
java -jar \  
$MW_HOME/discussionserver/discussionserver-upgradeforses.jar \  
<command_line_parameters>
```

where *command_line_parameters* are the following MDS schema details and discussions database schema details:

```
-mds_jdbc_user user_id \  
-mds_jdbc_password password \  
-mds_jdbc_url url \  
-discussions_jdbc_user user_id \  
-discussions_jdbc_password password \  
-discussions_jdbc_url url
```

where *mds_jdbc_user*, *mds_jdbc_password*, and *mds_jdbc_url* are the values to log in to the MDS schema, and *discussions_jdbc_user*, *discussions_jdbc_password*, and *discussions_jdbc_url* are the values to log in to the discussions database schema.

For example:

```
java -jar \  
$MW_HOME/as11r1wc/discussionserver/discussionserver-upgradeforses.jar\  
-mds_jdbc_user foo \  
-mds_jdbc_password welcome1 \  
-mds_jdbc_url jdbc:oracle:thin:@host:port:SID \  
-discussions_jdbc_user foo \  
-discussions_jdbc_password welcome1 \  
-discussions_jdbc_url jdbc:oracle:thin:@host:port:SID
```

22.5.3 Setting Up Oracle SES to Search WebCenter Portal

The steps in this section must be performed in the Oracle SES administration tool.

The following steps are required:

1. [Section 22.5.3.1, "Logging on to the Oracle SES Administration Tool"](#)
2. [Section 22.5.3.2, "Setting Up Oracle SES to Search Documents"](#)
3. [Section 22.5.3.3, "Setting Up Oracle SES to Search Discussions and Announcements"](#)
4. [Section 22.5.3.4, "Additional Oracle SES Configuration"](#)

See Also: Confirm that you have installed all required patches for Oracle SES. For the latest information on required patches, see "Back-End Requirements for the Search Service" in *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Portal* and the Release Notes.

For detailed information about Oracle SES configuration, see the Oracle SES documentation included with the product. (This is listed in the WebCenter Portal product area on the Oracle Fusion Middleware documentation library.)

22.5.3.1 Logging on to the Oracle SES Administration Tool

Open the Oracle SES administration tool:

1. Open a browser and enter the URL provided after the installation. (This has the form `http://host:port/search/admin/index.jsp`.)
2. Log on with the Oracle SES admin user name `eqsys` and the password specified during installation.

22.5.3.2 Setting Up Oracle SES to Search Documents

To search WebCenter Portal documents using Oracle SES, you must first set up a Document Service Manager (with a Document Service Instance and a Document Service Pipeline), and then create a Content Server source.

1. Configure the Document Service Manager (one time for each Oracle SES instance).

Note: Document services are plug-ins involved in the processing of a document when it is being crawled. A document service allows WebCenter Portal to add indexable attributes for documents used in the application.

Search attribute names must be unique; two attributes cannot have the same name. For example, if an attribute exists with a String data type, and another attribute is discovered by the crawler with the same name but a different data type, then the crawler ignores the second attribute. Before creating new attributes, make sure to check the list of Oracle SES attribute names and types in the Oracle SES documentation.

- a. On the Global Settings - Document Services page, click **Create**. Select **Create New Manager**, click **Next**, and enter the following parameters:

Manager Class Name:

`oracle.webcenter.search.crawl.ucm.ses.WcUcmDsManager`

Manager Jar File Name: `search-crawl-ucm.jar`

Note: The `webcenter_search_ses_plugins.zip` file installs `Oracle_Home/search/lib/plugins/doc/search-crawl-ucm.jar`.

Click **Next**, and then click **Finish** (Figure 22-13).

Figure 22–13 Creating a Document Services Manager in Oracle SES

ORACLE Secure Enterprise Search Search Help Logout

Home Search Global Settings

Global Settings > Document Services

Create Document Service Manager

Specify the class name and jar file for this document service manager. Cancel Next

- Manager Class Name (example: SampleDocManager)
- Manager Jar File Name (example: doc_plugins.jar)

TIP The jar file must be placed in the search/lib/plugins/doc directory, under the Oracle Secure Enterprise Search installed location. Cancel Next

b. Create the Document Service Instance.

Again, on the Global Settings - Document Services page, click **Create**. This time, select **Select From Available Managers with Secure Enterprise Search WebCenter UCM Plugin**, and click **Next** (Figure 22–14).

Figure 22–14 Create Document Service

ORACLE Secure Enterprise Search Search Help Logout

Home Search Global Settings

Global Settings > Document Services

Create Document Service

Document Service Manager Cancel

Create New Manager
 Select From
 Available Managers

Cancel

In addition to the entering an instance name, enter the following parameters:

WebCenter Application Name: This must be left blank.

Connection Name: The Content Server connection name in your WebCenter Portal application.

WebCenter URL Prefix: The host and port where the WebCenter Portal application is deployed, plus the context root; for example:
 http://myhost:8888/DocumentServer, where DocumentServer is the context root of the application.

c. Create the Document Services Pipeline. This invokes the document service instance.

Again, on the Global Settings - Document Services page, under the **Document Services Pipelines** section, click **Create**.

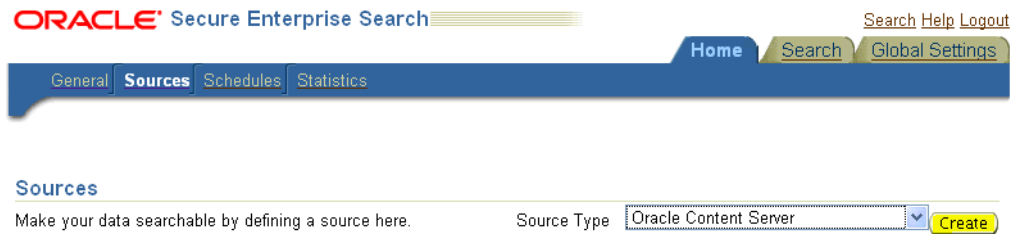
Enter a name and select the instance created in the previous step.

2. Create the Content Server source for documents.

a. Go to Home > Sources.

- b. From the Source Type dropdown list, select **Oracle Content Server**, and click **Create** (Figure 22–15).

Figure 22–15 Create Oracle Content Server Source



- c. Enter the following parameters:

Source Name: *unique_name*

Configuration URL: *Content_Server_SES_Crawler_Export_endpoint*;
for example,

`http://host:port/cs/idcplg?IdcService=SES_CRAWLER_DOWNLOAD_CONFIG&source=default`

Note: The `source=default` parameter denotes the name of the source created in the configuration of the SES Crawler Export. The default one is created automatically and called "default."

Authentication Type:

If the Content Server is not protected by SSO, then enter `NATIVE`.

If the Content Server is protected by Oracle SSO, then enter `ORASSO`.

User ID: The user to crawl the Content Server must have the `sceCrawlerRole` role defined. The `sceCrawlerRole` is a configuration parameter in `SESCrawlerExport`. Typically, administrators create a special role, assign it no privileges to view content, then create a user account that has this role.

If you do not set up a specific `sceCrawlerRole`, then admin credentials are required to crawl. The `sysadmin` user ID works by default.

If Authentication Type is `ORASSO`, then enter a user ID (and password) of a user in the identity management server fronted by Oracle SSO. This user must have been granted the same permissions as `sysadmin`. If it is not possible to grant those permissions, then delete the "remote" user corresponding to this user in the Content Server, and create a "local" version of the user (same name) in the Content Server.

Password: Password for this Content Server user.

Realm:

If Authentication Type is `NATIVE`, then enter `Idc Security /cs/idcplg`, where `/cs/` is the context root you provided when you installing the Content Server.

If Authentication Type is `ORASSO`, then leave this parameter blank.

Scratch Directory: Optional. Specify a directory on the system under which the Oracle SES instance resides.

Oracle SSO Login URL:

If Authentication Type is ORASSO, then specify a value for Oracle SSO. For example:

`https://login.oracle.com/mysso/signon.jsp?site2pstoretoken =`

If Authentication Type is NATIVE, then leave this field blank.

Oracle SSO Action URL:

If Authentication Type is ORASSO, then specify a value for Oracle SSO. For example: `https://login.oracle.com/sso/auth`

If Authentication Type is NATIVE, then leave this field blank.

Click **Next** (Figure 22–16).

Figure 22–16 Oracle Content Server Source Parameters

ORACLE Secure Enterprise Search Search Help Logout

Home Search Global Settings

General Sources Schedules Statistics

Home > Sources

Create User-Defined Source : Step 1 : Parameters Cancel Next

Source Name
 Source Type **Oracle Content Server**

Name	Value	Description
Configuration URL	<code>rice=SES_CRAWLER_DOWNLOAD_CONFIG&source=default</code>	File/HTTP URL of the configuration file
Authentication Type	NATIVE	Standard Java authentication type used by the application serving the control and data feed. This parameter is relevant when the feeds are accessed over HTTP. Enter BASIC for basic authentication, FORM for form-based authentication, ORASSO for Oracle SSO, NATIVE for proprietary XML over HTTP authentication.
User ID	sysadmin	User ID for accessing feeds
Password	••••••••	Password for accessing feeds
Realm	Idc Security /cs/idcplg	Realm of the application serving the control and data feed. This parameter is relevant when the feeds are accessed over HTTP and is mandatory when the authentication type is BASIC.
Oracle SSO Login URL		Oracle SSO login URL protecting all SSO applications. This parameter is relevant when the authentication type is ORASSO.
Oracle SSO Action URL		Oracle SSO action URL authenticating SSO user credentials. This is the URL to which the SSO login form is submitted. This parameter is relevant when the authentication type is ORASSO.
Scratch Directory		Local directory where status files can be temporarily written
Maximum number of connection attempts	3	Maximum number of connection attempts to access data feed or upload status feed

- d. On the Create User-Defined Source : Step 2 : Authorization page, enter the following parameters in the Authorization Manager section, if not entered by default:

Plug-in Class Name:

`oracle.search.plugin.security.auth.stellent.StellentAuthManager`

Jar File Name: `oracleapplications/StellentCrawler.jar`

HTTP endpoint for authorization: for example,

`http://host:port/cs/idcplg`

Display URL Prefix: for example, `http://host:port/cs`

Authentication Type: NATIVE or ORASSO

Administrator User: The user to crawl the Content Server must have the `sceCrawlerRole` role defined. The `sceCrawlerRole` is a configuration parameter in `SESCrawlerExport`. Typically, administrators create a special role, assign it no privileges to view content, then create a user account that has this role.

If you do not set up a specific `sceCrawlerRole`, then admin credentials are required to crawl. The `sysadmin` user ID works by default.

If Authentication Type is ORASSO, then enter a user ID (and password) of a user in the identity management server fronted by Oracle SSO. This user must have been granted the same permissions as `sysadmin`. If it is not possible to grant those permissions, then delete the "remote" user corresponding to this user in the Content Server, and create a "local" version of the user (same name) in the Content Server.

Administrator Password: Password for crawl admin user

Authorization User ID Format: Authentication attribute used in the active identity plug-in. To find this value, go to the Global Settings - Identity Management Setup page in Oracle SES. Enter the value of the Authentication Attribute under the Active Plug-in (for example, `nickname` or `username` or something else). If you are using the Oracle E-Business Suite R12 identity plug-in, then leave the this parameter blank.

Realm:

If Authentication Type is NATIVE, then enter "`Idc Security /cs/idcplg`", where `/cs/` is the context root you provided when you installing the Content Server.

In Authentication Type is ORASSO, then leave this field blank.

- e. Click **Create & Customize** (or edit a created source) to see other source parameters. On the **Crawling Parameters** tab, enter the following crawling parameter: `Document Service Pipeline`.
- f. Click **Enable** and select the pipeline you created.

22.5.3.3 Setting Up Oracle SES to Search Discussions and Announcements

To search WebCenter Portal's discussions and announcements using Oracle SES, you must first set up two Oracle SES Database sources: one for discussions and one for announcements. For example, the discussions source could have the source name `GS_Discussions` and a View of `FORUMCRAWLER_VW`, and the announcements source might have the source name `GS_Announcements` and a View of `ANNOUNCEMENTS_VW`.

Note: There are slightly different steps for Oracle, Microsoft SQL Server, and IBM DB2 databases.

1. Configure the JDBC driver:
 - a. To crawl a Microsoft SQL Server or IBM DB2 database, download the appropriate JDBC driver jar files into the

ORACLE_HOME/search/lib/plugins/oracleapplications directory in Oracle SES.

Note:

- For Microsoft SQL Server: Copy the Microsoft JDBC driver files `sqljdbc.jar` and `sqljdbc4.jar`.
 - For IBM DB2: Copy the IBM driver files `db2jcc.jar` and `db2jcc_license_cu.jar` (obtainable from the IBM DB2 UDB client).
-
-

If the JDBC drivers for JRE 1.5 and JRE 1.6 are different (for example: `sqljdbc.jar` works for JRE 1.5 and `sqljdbc4.jar` works for JRE 1.6), then perform the following:

- Download both the driver jars into the *ORACLE_HOME*/search/lib/plugins/oracleapplications directory in Oracle SES.

- Add an entry for the JRE 1.6 version (`sqljdbc4.jar` for SQLServer) of the driver jar to the CLASSPATH element of *ORACLE_HOME*/search/config/searchctl.conf.

- Restart the middle tier.

- b.** Update the `drivers.properties` file with the following information:
DatabaseName:DriverClassName.

- c.** Add the JRE 1.5 JDBC driver jar file name to the classpath in `META-INF/MANIFEST.MF` of `appsjdbc.jar` and `DBCrawler.jar`.

For example, change:

```
Class-Path: sqljdbc.jar rsscrawler.jar ../../pluginmessages.jar
```

to

```
Class-Path: db2jcc.jar sqljdbc.jar rsscrawler.jar
../../pluginmessages.jar
```

and change:

```
Class-Path: appsjdbc.jar
```

to

```
Class-Path: db2jcc.jar appsjdbc.jar
```

For a key attribute that is not named `KEY`, change the JDBC driver information in the `drivers.properties` file to specify the key attribute name:

```
database_name: driver_class_name, key_attribute_name
```

For example, for a key attribute named `ID`:

```
oracle : oracle.jdbc.driver.OracleDriver, ID
```

In the crawling query, use *key_attribute_name* as the alias for the key value column name. In this example, `ID` is the alias for `KEYVAL`:

```
SELECT keyval id, content, url, lastmodifieddate, lang FROM sales_only
```

Oracle and SQL Server databases: The following default drivers are used if none is specified in `drivers.properties`:

- Oracle: `oracle.jdbc.driver.OracleDriver`
- SQL Server: `com.microsoft.sqlserver.jdbc.SQLServerDriver`

2. Required for IBM DB2 databases only:

- a. Make sure that no crawlers are running that use the database crawler source. In the Oracle SES administration tool, check the crawler progress and status on the Home - Schedules page. (Click **Refresh Status**.)
- b. Remake the `appsjdbc.jar` file and the `DBCrawler.jar` file. Ensure that the `META-INF/MANIFEST.MF` was updated correctly; otherwise, the crawler fails with the following error in the crawler log file:

```
EQP-80406: Loading JDBC driver failed
```

- c. Modify the `Oracle_Home/search/lib/plugins/oracleapplications/drivers.properties` file to include the following line:

```
db2: com.ibm.db2.jcc.DB2Driver
```

- d. Include the driver jar (`db2jcc.jar`) to the `CLASSPATH` element of `ORACLE_HOME/search/config/searchctl.conf`. For example:

```
#CLASS PATH
CLASSPATH=ORACLE_HOME/search/webapp/config:ORACLE_HOME/search/webapp/
SESAuthenticator.jar:ORACLE_HOME/search/lib/plugins/commons-plugins-
stubs.jar :ORACLE_HOME /search/lib/plugins/oracleapplications/db2jcc.jar
```

- e. Edit `JVM_OPTIONS` in the `$ORACLE_HOME/search/config/searchctl.conf` file to add the system property `"-Doracle.home=ORACLE_HOME/search"`. For example:

```
JVM_OPTIONS= -Djava.awt.headless=true
-Dweblogic.RootDirectory=ORACLE_HOME/search/base_domain
-Doracle.home=ORACLE_HOME/search
```

- f. Copy the `$ORACLE_HOME/search/lib/plugins/oracleapplications/pluginmessages.jar` file to the `$ORACLE_HOME/search/lib` directory.
- g. Create the database source. Make sure to enter the correct authorization query and confirm that the attribute name used in **Grant Security Attributes** matches the one used in the authorization query; otherwise, users do not get any results when searching for documents.

3. Create a Discussions source or an Announcements source.

- a. In Oracle SES, go to **Home > Sources**.
- b. From the Source Type dropdown list, select **Database**, and click **Create** (Figure 22-17).

Figure 22–17 Create Database Source



c. Enter the following parameters:

Source Name: *unique_name*; for example, *GS_Discussions* to crawl discussions (or *GS_Announcements* to crawl announcements)

Database Connection String: Enter one of the following

- Oracle databases: Enter one of the following

```
jdbc:oracle:thin:@host:port:sid
```

```
jdbc:oracle:thin@host:port/serviceId
```

- IBM DB2 databases: Enter `jdbc:db2://host:port/database_name`

- Microsoft SQL Server databases: Enter

```
jdbc:sqlserver://host_or_IP_address:port;database_name
```

User ID: Enter one of the following:

- Oracle databases: The user *MyPrefix_DISCUSSIONS_CRAWLER* created during Oracle WebCenter Portal's Discussion Server installation

- Microsoft SQL Server databases: The user *MyPrefix_DISCUSSIONS_CRAWLER* created during Oracle WebCenter Portal's Discussion Server installation

- IBM DB2 databases: The user *MyPrefix_DC* created during Oracle WebCenter Portal's Discussion Server installation (where *MyPrefix* is five characters)

Password: Password for this user

Query: Enter one of the following queries:

```
SELECT * FROM FORUMCRAWLER_VW
SELECT * FROM ANNOUNCECRAWLER_VW
```

Use `FORUMCRAWLER_VW` for the source crawling discussion forums.

Use `ANNOUNCECRAWLER_VW` for the source crawling announcements.

URL Prefix: The URL prefix for the WebCenter Portal application, including host, port, and application name. For example, `http://host:port/webcenter`.

Grant Security Attributes: `WCSECATTR`

Note: Previous releases of Content Server used `FORUMID` for **Grant Security Attributes**.

d. Click **Next**.

- e. On the Create User-Defined Source : Step 2 : Authorization page, enter the following parameters (if not prepopulated) in the Authorization Manager section:

Plug-in Class Name:

`oracle.search.plugin.security.auth.db.DBAuthManager`

Jar File Name: `oracleapplications/DBCrawler.jar`

Authorization Database Connection String: Enter one of the following:

- Oracle databases: Enter one of the following:

`jdbc:oracle:thin:@host:port:sid`

`jdbc:oracle:thin@host:port/serviceId`

- IBM DB2 databases: Enter `jdbc:db2://host:port/database_name`

- Microsoft SQL Server databases: Enter

`jdbc:sqlserver://host_or_IP_address:port;database_name`

User ID: Enter one of the following:

- Oracle databases: Enter the user `MyPrefix_DISCUSSIONS_CRAWLER`

- Microsoft SQL Server databases: Enter the user

`MyPrefix_DISCUSSIONS_CRAWLER`

- IBM DB2 databases: Enter the user `MyPrefix_DC` (where `MyPrefix` is five characters)

Password: This user password

Single Record Query: `false`

Authorization Query: Enter the following (on one line):

```
SELECT DISTINCT forumID as WCSECATTR
FROM AUTHCRAWLER_FORUM_VW
WHERE username = ? UNION SELECT DISTINCT -1 as WCSECATTR
FROM AUTHCRAWLER_FORUM_VW
```

Note: Previous releases of Content Server used the following authorization query:

```
SELECT forumID
FROM AUTHCRAWLER_FORUM_VW
WHERE (username = ? or userID=-1)
UNION SELECT f.forumID
FROM jiveForum f, AUTHCRAWLER_CATEGORY_VW c
WHERE f.categoryID = c.categoryID AND (c.username = ? or
userID=-1)
```

Authorization User ID Format: Authentication attribute used in the active identity plug-in. To find this value, go to the Global Settings - Identity Management Setup page in Oracle SES. Enter the value of the Authentication Attribute under the Active Plug-in (for example, `nickname` or `username` or something else).

If you are using the Oracle E-Business Suite R12 identity plug-in, then leave the this parameter blank.

- f. Click **Create** to complete the source creation.

22.5.3.4 Additional Oracle SES Configuration

This section describes the required steps in the Oracle SES administration tool.

1. Create a *source group* that includes the names of the Content Server, Discussions, Announcements, and WebCenter Portal services sources you created.
 - a. Go to the Search - Source Groups page, and click **Create**.
 - b. Enter the same source group name entered in [Section 22.5.4, "Setting Up WebCenter Portal: Framework for Oracle SES Search."](#)
 - c. From the **Select Source Type** dropdown list, select each source type (Database, Oracle Content Server, Oracle WebCenter), and then from the Available Sources listed for each source type, move the source you created for that source type into the Assigned Sources list.
 - d. Click **Finish**.
2. Optionally configure the security filter lifespan. This refreshes the authorization policies for users in the system. It is best to have a short lifespan when user policies change frequently. (This chapter uses Oracle Internet Directory identity plug-in as the example.)

For example, on the Global Settings - Query Configuration page, under **Secure Search Configuration**, enter 0 for **Security Filter Lifespan (minutes)**.

Valid values for the security filter lifespan are between 0 minutes (no cache) and 526500 minutes (cache for one year).

3. To index everything, you must force a full crawl for each source; that is, you must change the existing incremental crawl schedule for each source to first process ALL documents.

This step is very important, in that searching does not work unless the content is first indexed completely.

Go to the Home - Schedules page, select the source schedule, and click **Edit** to force a full crawl.

After each source has been crawled, go back to the same page and change the crawl policy back to incremental (index documents that have changed since the previous crawl). Also, in the Frequency section of the page, select a non-manual type for running incremental crawl (for example, weekly or daily).

Note: Before the first crawl of the Content Server, remember to go to the Content Server Administration page, select **SES Crawler Export**, and take a snapshot. For more information, see [Section 22.5.1, "Setting Up Oracle WebCenter Portal Content Server for Oracle SES Search."](#)

22.5.4 Setting Up WebCenter Portal: Framework for Oracle SES Search

This section describes how to configure WebCenter Portal: Framework to work with Oracle SES.

Make sure you have created and configured the connection between WebCenter Portal and Oracle SES, specifying the Federation Trusted Entity, and optionally specifying a source group.

The Oracle SES crawlers are enabled by default in Framework applications.

See Also: "Setting Up Connections for the Search Service" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*

22.5.4.1 Configuring Framework Applications After Deployment

After a Framework application has been deployed to an Oracle WebLogic managed server, you can configure it using WLST or Fusion Middleware Control. This section contains the following subsections:

- [Section 22.5.4.1.1, "Modifying Search Parameters Using WLST"](#)
- [Section 22.5.4.1.2, "Configuring Search Crawlers Using WLST"](#)
- [Section 22.5.4.1.3, "Configuring Search Parameters and Crawlers Using Fusion Middleware Control"](#)

22.5.4.1.1 Modifying Search Parameters Using WLST Use the WLST command `setSearchConfig` to modify search parameters post deployment.

[Example 22–2](#) shows how to specify a data group (also known as source group) under which you search Oracle SES.

Example 22–2 Set a Source Group

```
setSearchSESConfig(appName='webcenter',
                  dataGroup='MySources')
```

where `dataGroup` is the source group you create in [Section 22.5.3.4, "Additional Oracle SES Configuration"](#) (for Framework applications) or in [Section 22.6.4.6, "Additional Oracle SES Configuration"](#) (for Spaces applications).

[Example 22–3](#) shows how to increase the number of search results displayed. Five is the default setting for the number of search results displayed in Oracle SES results, but result sets generally are larger than five.

Example 22–3 Increase Number of Search Results Displayed

```
setSearchConfig(appName='webcenter',
                numResultsMain=10)
```

[Example 22–4](#) shows how to configure the maximum time that a service is allowed to execute a search (in ms). When a service times out largely depends on the system load. If you consistently get time out errors, adjust this parameter.

Example 22–4 Configure Maximum Time WebCenter Waits for Search Results

```
setSearchConfig(appName='webcenter',
                executionTimeout=10000)
```

For command syntax and examples, see the section, "setSearchConfig" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

22.5.4.1.2 Configuring Search Crawlers Using WLST You can use WLST commands to create crawlers and to start, stop and delete crawler schedules post deployment. These commands let you crawl new data in Oracle SES or delete old crawlers if the configuration data changes.

[Example 22–5](#) and [Example 22–6](#) show some of these commands. For more information, see the section, "Search - Oracle SES Search Crawlers" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

Example 22-5 Create a Documents Crawler in WLST

```
createDocumentsCrawler(
'portal', 'portal_host', 'portal_port',
'http://ses-host:ses-port/search/api/admin/AdminService', 'ses-admin-pw',
'http://ucm-host:ucm-port/cs/idcplg?IdcService=
SES_CRAWLER_DOWNLOAD_CONFIG&source=default', 'ucm-crawl-user',
'ucm-crawl-user-pw', '/tmp',
'http://ucm-host:ucm-port/cs/idcplg', 'http://ucm-host:ucm-port/cs',
'Idc Security /cs/idcplg', 'authentication-id-format', 'Document-pipeline',
'ACCEPT_ALL', 'PROCESS_CHANGED', 'MANUAL', 1, 1, 'MONDAY', 1, 1, 1, 1)
```

where:

- *portal* = Name of the Framework application in which to perform this operation
- *portal_host* = Host name of the system where the Framework application is running
- *portal_port* = Port number used to access the Framework application
- *ses-host* = Oracle SES host name
- *ses-port* = Oracle SES port number
- *ses-admin-pw* = Oracle SES admin user password
- *ucm-host* = Content Server host name
- *ucm-port* = Content Server port number
- *ucm-crawl-user* = Content Server crawl user name
- *ucm-crawl-user-pw* = Content Server crawl user password
- *authentication-id-format* = Use 'nickname' if the Identity Management plug-in on Oracle SES is set to Oracle Internet Directory; otherwise, use the value of the **Authentication Attribute** parameter on the Identity Management plug-in on Oracle SES
- *Document-pipeline* = Document pipeline on Oracle SES created for this Framework instance

Example 22-6 Create a Discussions Crawler in WLST

```
createDiscussionsCrawler(
'webcenter', 'webcenter_host', 'webcenter_port',
'http://ses-host:ses-port/search/api/admin/AdminService', 'ses-admin-pw',
'jdbc:oracle:thin:@database-host:database-port:database-sid',
'Jive-crawler-schema', 'Jive-crawler-schema-pw', 'authentication-id-format',
'ACCEPT_ALL', 'PROCESS_ALL', 'MANUAL', 1, 1, 'MONDAY', 1, 1, 1, 1)
```

where:

- *webcenter_host* = Framework application host name
- *webcenter_port* = Framework application port number
- *ses-host* = Oracle SES host name
- *ses-port* = Oracle SES port number
- *ses-admin-pw* = Oracle SES admin user password
- *database-host* = Discussions server database host name
- *database-port* = Discussions server database port number

- `database-sid` = Discussions server database name or SID
- `Jive-crawler-schema` = Discussions server crawler schema name. Determine the prefix from RCU, and use `rcu-prefix_DISCUSSION_CRAWLER`.
- `Jive-crawler-schema-pw` = Discussions server crawler schema password
- `authentication-id-format` = Use 'nickname' if the Identity Management plug-in on Oracle SES is set to Oracle Internet Directory; otherwise, use the value of the **Authentication Attribute** parameter on the Identity Management plug-in on Oracle SES.

Note: To effect WLST changes, you must restart the managed server on which the WebCenter Portal application is deployed (by default, WC_Spaces). For more information, see the section "Starting and Stopping WebLogic Managed Servers Using the Command Line" in *Oracle Fusion Middleware Administrator's Guide*.

22.5.4.1.3 Configuring Search Parameters and Crawlers Using Fusion Middleware Control You can enable or disable Oracle SES search and configure search settings using Fusion Middleware Control.

1. Log in to Fusion Middleware Control and navigate to the home page for your WebCenter Portal application. For more information, see [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#) or [Section 6.3, "Navigating to the Home Page for Framework Applications."](#)
2. From the **WebCenter Portal** menu, choose **Settings > Application Configuration**.
3. Select to enable the Oracle SES adapter or the default WebCenter Portal adapters, and click **Apply** (Figure 22–18).

Optionally, you can configure search parameters.

- **Oracle Secure Enterprise Search Data Group:** Specify the Oracle SES source group in which to search. If no value is provided, then everything in the Oracle SES instance is 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).
- **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. Users can click Show All if they want to see all the results.
- **Number of Saved Searches in Search Page:** Enter the number of saved searches displayed in the Saved Search list (on the main search page).

You do *not* need to restart the managed server on which the Framework application is deployed.

Figure 22–18 Application Settings for Oracle Search

Application Settings ?
Apply Revert

Search Crawlers

WebCenter Portal application content can be searched by WebCenter search adapters or Oracle Secure Enterprise Search (SES). Oracle SES is used by default and requires additional crawler configuration through Oracle SES Administration. To use WebCenter search adapters in your application, change the selection below.

Search Crawler Configuration Use WebCenter Search Adapters Use Oracle SES to Search the WebCenter Portal Application

Search Settings

Fine-tune WebCenter searches using these settings. Set suitable search timeouts for WebCenter services and specify how many search results to return and display.

Oracle Secure Enterprise Search Data Group	<input style="width: 100%;" type="text"/>
Execution Timeout (ms)	<input style="width: 50%;" type="text" value="3000"/>
Executor Preparation Timeout (ms)	<input style="width: 50%;" type="text" value="1000"/>
Results per Service - Saved Search Task Flows	<input style="width: 50%;" type="text" value="5"/>
Results per Service - Search Page	<input style="width: 50%;" type="text" value="5"/>
Number of Saved Searches in Search Page	<input style="width: 50%;" type="text" value="5"/>

22.6 Configuring Oracle SES to Search Spaces Applications

With Spaces applications, WebCenter Portal's internal live search adapters are set as the default search platform; however, large-scale implementations should be configured to use Oracle SES for best performance.

Note: For an overview of the tasks that must be performed to enable Oracle SES as the search engine in Spaces, see [Section 22.2, "Configuration Roadmaps for Oracle SES in WebCenter Portal."](#) There may be various acceptable ways and orders to perform the required tasks.

This section describes the steps necessary to set up Oracle SES to search Spaces:

- [Section 22.6.1, "Setting Up WebCenter Portal: Spaces for Oracle SES Search"](#)
- [Section 22.6.2, "Setting Up Oracle WebCenter Portal: Content Server for Oracle SES Search"](#)
- [Section 22.6.3, "Setting Up Oracle WebCenter Portal Discussion Server for Oracle SES Search"](#)
- [Section 22.6.4, "Setting Up Oracle SES to Search WebCenter Portal"](#)
- [Section 22.6.5, "Configuring Search Crawlers Using WLST"](#)

See Also: [Section 22.1, "What You Should Know About WebCenter Portal's Search with Oracle SES"](#)

22.6.1 Setting Up WebCenter Portal: Spaces for Oracle SES Search

This section describes how to configure WebCenter Portal: Spaces to work with Oracle SES.

1. Create and configure the connection between Spaces and Oracle SES, and optionally specifying a source group.

See Also: [Section 22.4.1.2, "Registering Oracle SES Connections Using WLST"](#) and [Section 22.4.3.2, "Modifying Oracle SES Connection Details Using WLST"](#)

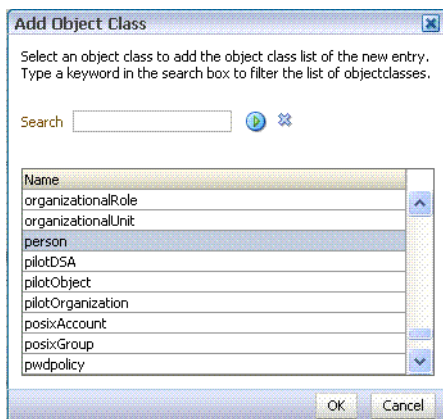
2. To use Oracle SES to search spaces, lists, or pages, you must first create a *crawl admin user* in WebCenter Portal: Spaces and in your back-end identity management server (for example, *mycrawladmin*). You must only create a crawl admin user once.

Note: See your identity management system documentation for information on creating users.

The following example uses Oracle Directory Services Manager to create the *mycrawladmin* user.

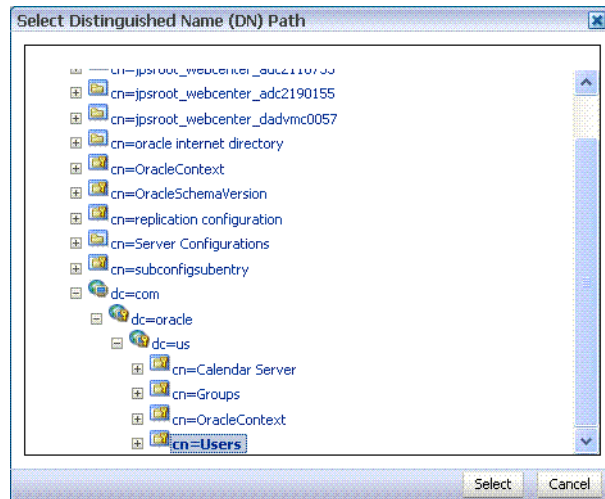
- a. On the Data Browser tab, navigate to the target *cn* and click **Create**. This example navigates to "dc=com,dc=oracle,dc=us,cn=Users". In the Add Object Class dialog, select the appropriate object class, and click **OK**. ([Figure 22–19](#)).

Figure 22–19 Oracle Directory Services Manager - Add Object Class



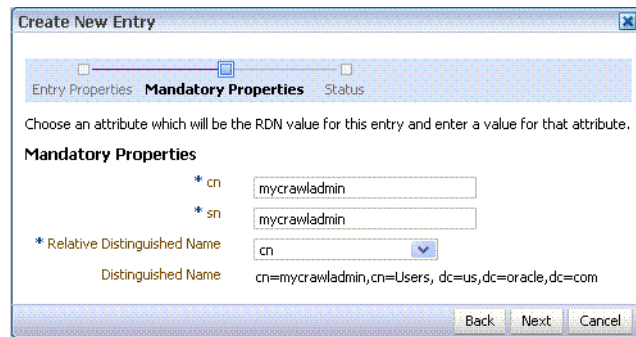
- b. Find the distinguished name (DN) path, and click **Select** ([Figure 22–20](#)). This example selects "dc=com,dc=oracle,dc=us,cn=Users".

Figure 22–20 Oracle Directory Services Manager - Select DN Path



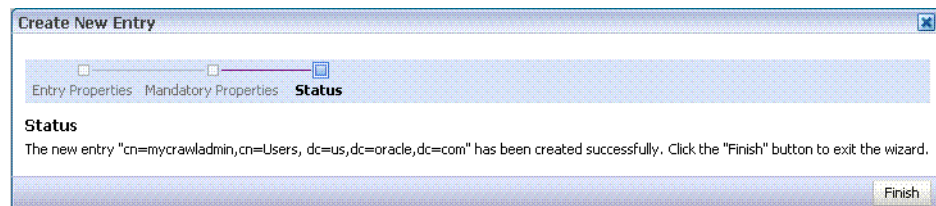
- c. In the Create New Entry dialog, enter properties, and click **Next** (Figure 22–21).

Figure 22–21 Oracle Directory Services Manager - Create New Entry



- d. When you see that the new entry was created successfully, click **Finish**. (Figure 22–22)

Figure 22–22 Oracle Directory Services Manager - Status



3. Create a *crawl* application role for WebCenter Portal: Spaces.
 - a. See if the crawl application role exists with the following command:

```
listAppRoles (appStripe='webcenter')
```

For command syntax and examples, see the section, "listAppRoles" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

The list may be very long. Look for 'webcenter#-#defaultcrawl' as a Principal Name in the results. For example:

```
[ [Principal Clz Name :
oracle.security.jps.internal.core.principals.JpsApplicationRoleImpl,
Principal Name :webcenter#-#defaultcrawl, Type : APP_ROLE], Display Name :
Crawl Role. This role never gets updated by webcenter UIs., Description :
null, Guid : DA91B6572AF911DFBF70237926348A3B]
```

If 'webcenter#-#defaultcrawl' does not exist, then you must create the crawl application role with the following WLST command:

```
createAppRole(appStripe='webcenter',
              appRoleName='webcenter#-#defaultcrawl');
```

For command syntax and examples, see the section, "createAppRole" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

Then grant "view" permissions to Spaces content as follows:

```
grantPermission(appStripe="webcenter",
principalClass="oracle.security.jps.service.policystore.ApplicationRole",
principalName="webcenter#-#defaultcrawl",
permClass="oracle.webcenter.community.model.security.CommunityPermission",
permTarget="*",
permActions="view")

grantPermission(appStripe="webcenter",
principalClass="oracle.security.jps.service.policystore.ApplicationRole",
principalName="webcenter#-#defaultcrawl",
permClass="oracle.webcenter.relationship.model.security.RelationshipPermission",
permTarget="*",
permActions="view")

grantPermission(appStripe="webcenter",
principalClass="oracle.security.jps.service.policystore.ApplicationRole",
principalName="webcenter#-#defaultcrawl",
permClass="oracle.webcenter.list.model.security.ListPermission",
permTarget="*",
permActions="view")

grantPermission(appStripe="webcenter",
principalClass="oracle.security.jps.service.policystore.ApplicationRole",
principalName="webcenter#-#defaultcrawl",
permClass="oracle.webcenter.page.model.security.CustomPagePermission",
permTarget="*",
permActions="view")

grantPermission(appStripe="webcenter",
principalClass="oracle.security.jps.service.policystore.ApplicationRole",
principalName="webcenter#-#defaultcrawl",
permClass="oracle.webcenter.page.model.security.PagePermission",
permTarget="*",
permActions="view")

grantPermission(appStripe="webcenter",
principalClass="oracle.security.jps.service.policystore.ApplicationRole",
principalName="webcenter#-#defaultcrawl",
permClass="oracle.webcenter.note.model.security.NotePermission",
permTarget="*",
```

```

permActions="view")

grantPermission(appStripe="webcenter",
principalClass="oracle.security.jps.service.policystore.ApplicationRole",
principalName="webcenter#-#defaultcrawl",
permClass="oracle.webcenter.collab.calendar.model.security.EventPermission"
,
permTarget="*",
permActions="view")

```

For command syntax and examples, see the section, "grantPermission" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

- b. Grant the crawl application role to the crawl admin user created in [Section 22.3.2, "Oracle SES - Configuration."](#) For example:

```

grantAppRole(appStripe="webcenter",
             appRoleName="webcenter#-#defaultcrawl",
             principalClass="weblogic.security.principal.WLSUserImpl",
             principalName="mycrawladmin");

```

For command syntax and examples, see the section, "grantAppRole" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

Note: To effect WLST changes, you must restart the managed server on which the application is deployed (by default, WC_Spaces). For more information, see the section "Starting and Stopping WebLogic Managed Servers Using the Command Line" in *Oracle Fusion Middleware Administrator's Guide*.

4. Enable the Oracle SES crawlers in WebCenter Portal.

With the same WLST command, you can set crawler properties (that is, enable/disable the crawlers) and specify an interval between full crawls for the Spaces crawler. By default, full crawls for the Spaces crawler occur every seven days, but you can specify a different frequency. (Incremental crawls are initiated by the schedule set in Oracle SES.)

For example:

```

setSpacesCrawlProperties(appName='webcenter',
                        fullCrawlIntervalInHours=168,
                        spacesCrawlEnabled = true,
                        documentCrawlEnabled=true,
                        discussionsCrawlEnabled=true)

```

Notes: The `spacesCrawlEnabled`, `documentCrawlEnabled` and `discussionsCrawlEnabled` parameters all must be set to `true` to enable Oracle SES search.

A clustered instance additionally requires the `server` parameter; for example, `server="WC_Spaces1"`.

The following example specifies that Spaces runs a full crawl through the Spaces crawler every 8 days.

```

setSpacesCrawlProperties(appName='webcenter', fullCrawlIntervalInHours=192)

```

You also can use WLST to return the current crawl settings for WebCenter Portal, such as the number of hours between full crawls (Spaces crawler). For example, the following command returns the current crawl settings for Spaces.

```
getSpacesCrawlProperties (appName='webcenter')
```

```
WebCenter Spaces Crawl Properties:
```

```
-----
```

```
fullCrawlIntervalInHours: 124
spacesCrawlEnabled:      true
documentCrawlEnabled:   true
discussionsCrawlEnabled: true
```

5. Use the `listDocumentsSpacesProperties` command to determine the unique name that the back-end Content Server is using to identify this WebCenter Portal application and the connection name for the primary Content Server that WebCenter Portal is using to store documents. For example:

```
listDocumentsSpacesProperties (appName='webcenter')
```

The response should look something like the following:

```
The Documents Spaces container is "/WebCenter1109"
The Documents repository administrator is "sysadmin"
The Documents application name is "WC1109"
The Documents primary connection is "stxxl18-ucm11g"
```

Note: Record the application name and the primary connection returned. These values are required later (in [Section 22.6.4.2, "Setting Up Oracle SES to Search Documents"](#)) to set up Oracle SES to crawl documents.

Note: To effect WLST changes, you must restart the managed server on which the application is deployed (by default, WC_Spaces). For more information, see the section "Starting and Stopping WebLogic Managed Servers Using the Command Line" in *Oracle Fusion Middleware Administrator's Guide*.

22.6.1.1 Configuring Search Parameters Using WLST

Use the WLST command `setSearchConfig` to modify search parameters.

[Example 22-7](#) shows how to specify a data group (also known as source group) under which you search Oracle SES.

Example 22-7 Set a Source Group

```
setSearchSESConfig (appName='webcenter',
                   dataGroup='MySources')
```

where `dataGroup` is the source group you create in [Section 22.5.3.4, "Additional Oracle SES Configuration"](#) (for Framework applications) or in [Section 22.6.4.6, "Additional Oracle SES Configuration"](#) (for Spaces applications).

[Example 22-8](#) shows how to increase the number of search results displayed. Five is the default setting for the number of search results displayed in Oracle SES results, but result sets generally are larger than five.

Example 22–8 Increase Number of Search Results Displayed

```
setSearchConfig (appName='webcenter',
                 numResultsMain=10)
```

[Example 22–9](#) shows how to configure the maximum time that a service is allowed to execute a search (in ms). When a service times out largely depends on the system load. If you consistently get time out errors, adjust this parameter.

Example 22–9 Configure Maximum Time WebCenter Portal Waits for Search Results

```
setSearchConfig (appName='webcenter',
                 executionTimeout=10000)
```

For command syntax and examples, see the section, "setSearchConfig" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

22.6.1.2 Configuring Search Parameters and Crawlers Using Fusion Middleware Control

You can enable or disable Oracle SES search and configure search settings using Fusion Middleware Control.

1. Log in to Fusion Middleware Control and navigate to the home page for your WebCenter Portal application. For more information, see [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#) or [Section 6.3, "Navigating to the Home Page for Framework Applications."](#)
2. From the **WebCenter Portal** menu, choose **Settings > Application Configuration**.
3. Select to enable the Oracle SES adapter or the default WebCenter Portal search adapters, and click **Apply** ([Figure 22–23](#)).

You can specify an interval between full crawls for the Spaces crawler. By default, full crawls for the Spaces crawler occur every seven days, but you can specify a different frequency. (Incremental crawls, for all three crawlers, are initiated by the schedule set in Oracle SES.)

Optionally, you can configure search parameters.

- **Oracle Secure Enterprise Search Data Group:** Specify the Oracle SES source group in which to search. If no value is provided, then everything in the Oracle SES instance is 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).
- **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. Users can click Show All if they want to see all the results.
- **Number of Saved Searches in Search Page:** Enter the number of saved searches displayed in the Saved Search list (on the main search page).

You do *not* need to restart the managed server on which the WebCenter Portal application is deployed.

Figure 22–23 Application Settings for WebCenter Portal Search

Application Settings ?
Apply Revert

Spaces Workflows

The Spaces application uses the BPEL server included with the Oracle SOA Suite to implement space subscription workflows. Specify the connection that points to the correct SOA Suite deployment. Choose from a list of existing active workflow connections.

Connection Name Select a connection for Spaces workflows

Search Crawlers

Spaces content can be searched by WebCenter Portal search adapters or Oracle Secure Enterprise Search (SES). WebCenter Portal search adapters are used by default. To use Oracle SES in Spaces, change the selection below and configure crawlers through Oracle SES Administration. In addition, you can specify the Full Crawl Interval for internal WebCenter Portal content such as spaces, pages, lists, and people.

Search Crawler Configuration Use WebCenter Portal Search Adapters Use Oracle SES

Full Crawl Interval (hours)

Search Settings

Fine-tune WebCenter Portal searches using these settings. Set suitable search timeouts for WebCenter Portal services and specify how many search results to return and display.

Oracle Secure Enterprise Search Data Group	<input style="width: 100%;" type="text"/>
Execution Timeout (ms)	<input style="width: 60px;" type="text" value="7000"/>
Executor Preparation Timeout (ms)	<input style="width: 60px;" type="text" value="3000"/>
Results per Service - Saved Search Task Flows	<input style="width: 60px;" type="text" value="5"/>
Results per Service - Search Page	<input style="width: 60px;" type="text" value="10"/>
Number of Saved Searches in Search Page	<input style="width: 60px;" type="text" value="25"/>

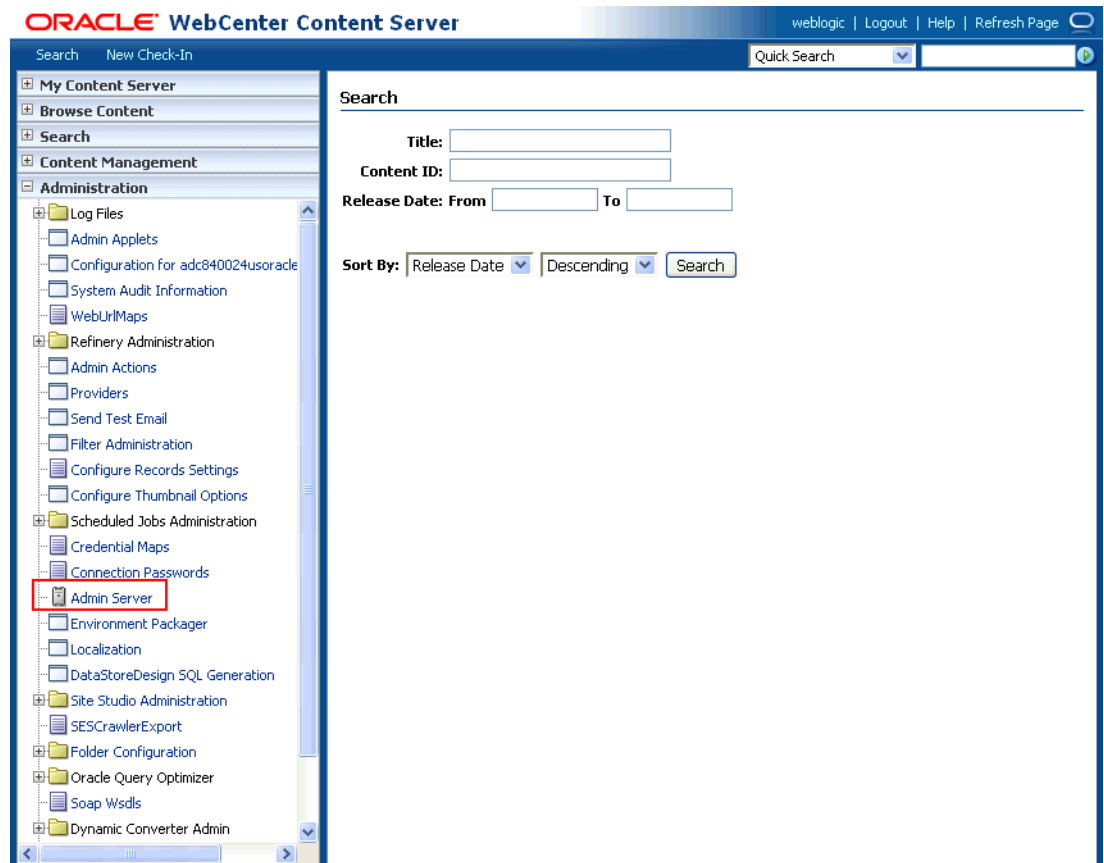
22.6.2 Setting Up Oracle WebCenter Portal: Content Server for Oracle SES Search

This section describes how to configure Oracle WebCenter Content: Content Server to be crawlable by Oracle SES (in particular, the Content Server that WebCenter Portal uses for storing documents).

The following steps must be done from within the Content Server.

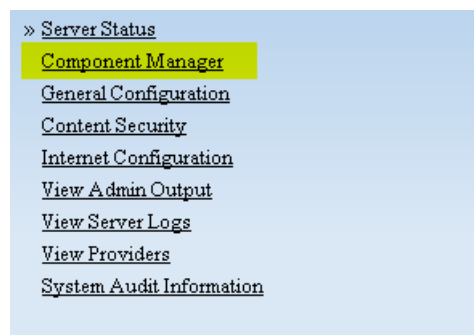
1. Create the role `sescrawlerrole`.
2. Create the user `sescrawler`, and assign it the `admin` role and the `sescrawlerrole` role. This user creates the Content Server source in Oracle SES.
3. Add `sceCrawlerRole=sescrawlerrole` to `config.cfg`.
4. Restart the Content Server.
5. In the Content Server console, install the `SESCrawlerExport` component on the content server, if not done:
 - a. Log on to the Content Server as a system administrator. For example: `http://host:port/cs`.
 - b. From the Administration dropdown menu, select **Admin Server** (Figure 22–24).

Figure 22–24 Content Server Administration



- c. Click the button with the instance name.
- d. Click **Component Manager** from the menu list on the left pane (Figure 22–25).

Figure 22–25 Content Server Component Manager



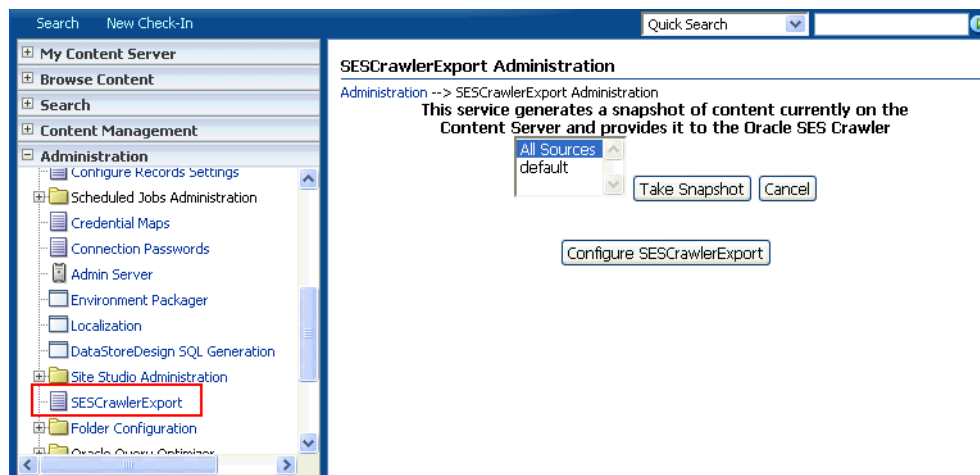
- e. Select **SESCrawlerExport** under Integration and click **Update**.
- f. Enter configuration parameters. (You can change configuration parameters after installation.)

Disable security on authentication and authorization APIs provided by the **SESCrawlerExport**; that is, set **Disable Secure APIs** to `false`. This lets security provided by the **SESCrawlerExport** be done internally instead of by the content server.

Additionally, in clustered environments only, the **feedLoc** parameter must specify a location on the shared disk accessed by the nodes of content server, and they each must reference it the same way; for example, `sharedDrive/dir1/dir2`. Note that this is not the default location (relative path) provided.

- g. Restart the Content Server.
6. Take a snapshot of the Content Server repository.
 - a. Log on to the Content Server as a system administrator. For example: `http://host:port/cs`.
 - b. From the Administration dropdown menu, select **SESCrawlerExport**.
 - c. Select **All sources**, and click **Take Snapshot** (Figure 22–26).

Figure 22–26 Content Server Snapshot



It is important to take a snapshot before the first crawl or any subsequent full crawl of the source.

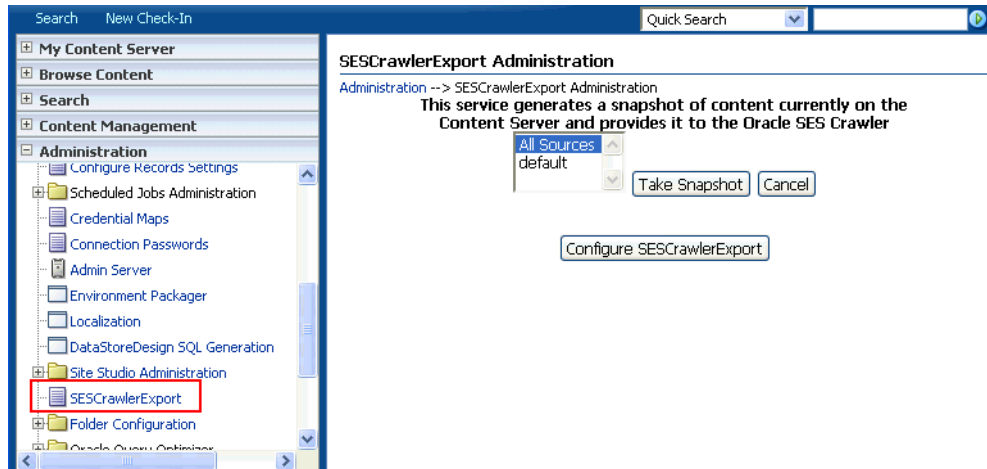
The snapshot generates `configFile.xml` at the location specified during component installation, and feeds are created at the subdirectory with the source name under **feedLoc**.

7. If the Content Server is configured for web rendition, then items in the Content Server are rendered in PDF format. The content item's native MIME type rendition is overwritten. For example, the MIME type of a Microsoft Office Word document is 'application/msword', but when the Content Server uses web rendition the MIME type becomes 'application/pdf'. A search query with the `Mimetype` parameter set to 'application/msword' does not return Word documents.

If your Content Server is configured to use web rendition, then you must configure the Content Server metadata list to include the `dFormat` value, so that required MIME types are exported to Oracle SES. This is necessary to be able to narrow searches by MIME type.

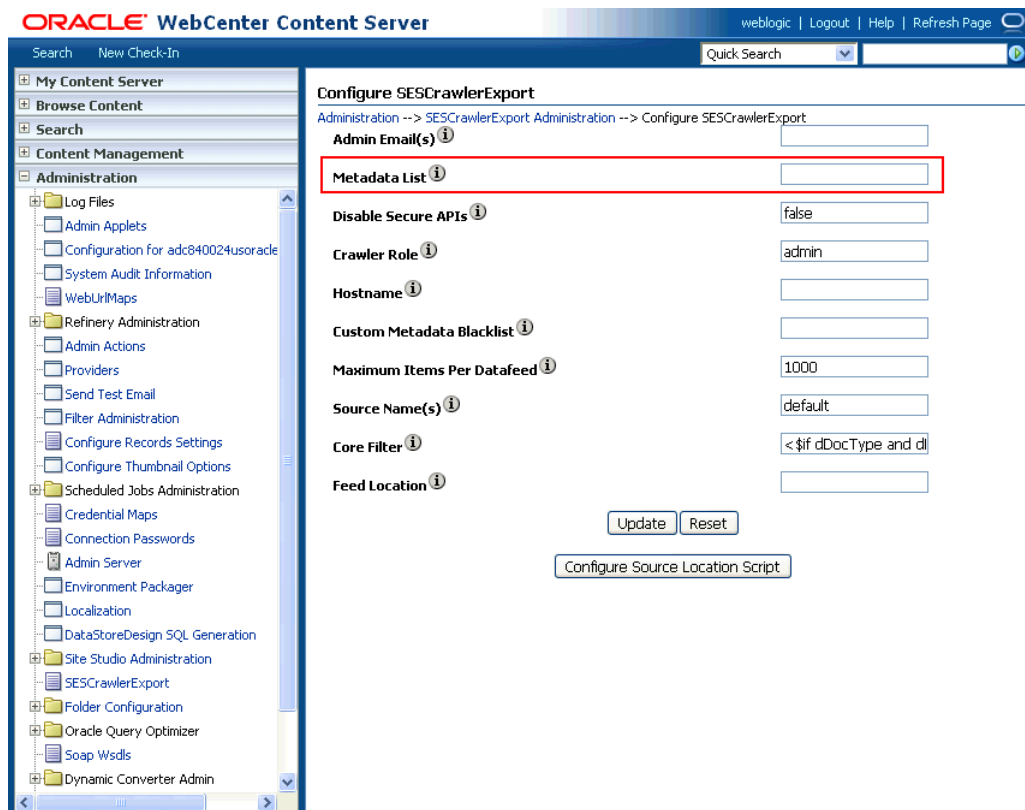
- a. Back on the SESCrawlerExport Administration page, click **Configure SESCrawlerExport** (Figure 22–11).

Figure 22–27 Content Server Snapshot



- b. By default, the Metadata List field is blank (Figure 22–28).

Figure 22–28 Content Server Metadata List



Left blank, the list of metadata values that are exported to Oracle SES consists of the following (plus any custom metadata fields beginning with 'x'):

dID, dDocName, dRevLabel, dDocType, dDocAccount, dSecurityGroup, dOriginalName, dReleaseDate, dOutDate

However, the dFormat value must be added to this list.

When the blank default value is changed, the default values are removed, so they also must be added back. Enter the value for **Metadata List** as follows:

dFormat, dID, dDocName, dRevLabel, dDocType, dDocAccount, dSecurityGroup, dOriginalName, dReleaseDate, dOutDate

- c. Optionally, add to this list any custom metadata values you require (beginning with x).

For example, the following entry for **Metadata List** includes custom attributes:

dFormat, dID, dDocName, dDocType, dDocAccount, dSecurityGroup, dOriginalName, dReleaseDate, dDocAuthor, dDocCreator, dDocCreatedDate, dOutDate, xCollectionID, xWCTags, xComments, xRegionDefinition

See Also:

- For information about displaying MIME types in search results, see "Customizing Search Results with Attributes and Refiners" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*
- For detailed information on Content Server configuration, see the *Deployment Guide.pdf* included with the product.

22.6.3 Setting Up Oracle WebCenter Portal Discussion Server for Oracle SES Search

This section describes how to configure Oracle WebCenter Portal's Discussion Server to be crawlable by Oracle SES (in particular, the discussions server that WebCenter Portal uses for storing discussions and announcements).

Note: These steps is not required if you have a new installation of WebCenter Portal (with an Oracle database) and Oracle WebCenter Portal's Discussion Server. It is only required if you are using upgraded (patched) instances.

You can find database schema details for the corresponding data sources from your Oracle WebLogic Server console.

1. Run the Repository Creation Utility (RCU) to confirm that the Discussions Crawler WebCenter Portal component has been installed on the system.
 - Oracle and Microsoft SQL Server databases:

Verify that the Oracle WebCenter Portal's Discussion Server back end has been configured properly by noting that the *MyPrefix_DISCUSSIONS* user is installed in RCU.

Then verify that the Discussions Crawler has been configured properly by noting that the *MyPrefix_DISCUSSIONS_CRAWLER* user is installed in RCU.
 - IBM DB2 databases:

Verify that the Oracle WebCenter Portal's Discussion Server back end has been configured properly by noting that the *MyPrefix_DS* user is installed in RCU.

Then verify that the Discussions Crawler has been configured properly by noting that the *MyPrefix_DC* user is installed in RCU.

Note: For IBM DB2 databases, *MyPrefix* is limited to five characters. IBM DB2 uses operating system users for authentication (that is, the database user is actually an operating system user). Because some operating systems have an eight character limit for user names, this requires an eight character user name.

If the Discussions Crawler component is not installed, then you must install it using RCU, selecting the same prefix that was used for the Oracle WebCenter Portal's Discussion Server component. Also, during the tablespace specification step in RCU, select *Prefix_IAS_DISCUSSIONS* as the default tablespace. This installs the user for Oracle SES.

For more information, see [Chapter 7, "Deploying WebCenter Portal: Framework Applications."](#)

2. Run the following tool to upgrade the data in the discussions server database schema, if you have not run the tool yet:

```
java -jar \  
$MW_HOME/discussionserver/discussionserver-upgradeforses.jar \  
<command_line_parameters>
```

where *command_line_parameters* are the following MDS schema details and discussions database schema details:

```
-mds_jdbc_user user_id \  
-mds_jdbc_password password \  
-mds_jdbc_url url \  
-discussions_jdbc_user user_id \  
-discussions_jdbc_password password \  
-discussions_jdbc_url url
```

where *mds_jdbc_user*, *mds_jdbc_password*, and *mds_jdbc_url* are the values to log in to the MDS schema, and *discussions_jdbc_user*, *discussions_jdbc_password*, and *discussions_jdbc_url* are the values to log in to the discussions database schema.

For example:

```
java -jar \  
$MW_HOME/as11r1wc/discussionserver/discussionserver-upgradeforses.jar \  
-mds_jdbc_user foo \  
-mds_jdbc_password welcome1 \  
-mds_jdbc_url jdbc:oracle:thin:@host:port:SID \  
-discussions_jdbc_user foo \  
-discussions_jdbc_password welcome1 \  
-discussions_jdbc_url jdbc:oracle:thin:@host:port:SID
```

22.6.4 Setting Up Oracle SES to Search WebCenter Portal

The steps in this section must be performed in the Oracle SES administration tool.

The following steps are required:

1. [Section 22.6.4.1, "Logging on to the Oracle SES Administration Tool"](#)
2. [Section 22.6.4.2, "Setting Up Oracle SES to Search Documents"](#)
3. [Section 22.6.4.3, "Setting Up Oracle SES to Search Discussions and Announcements"](#)

4. [Section 22.6.4.4, "Setting Up Oracle SES to Search Spaces, Lists, Pages, and People"](#)
5. [Section 22.6.4.6, "Additional Oracle SES Configuration"](#)

See Also: Confirm that you have installed all required patches for Oracle SES. For the latest information on required patches, see "Back-End Requirements for the Search Service" in *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Portal* and the Release Notes.

For detailed information about Oracle SES configuration, see the Oracle SES documentation included with the product. (This is listed in the WebCenter Portal product area on the Oracle Fusion Middleware documentation library.)

22.6.4.1 Logging on to the Oracle SES Administration Tool

Open the Oracle SES administration tool:

1. Open a browser and enter the URL provided after the installation. (This has the form `http://host:port/search/admin/index.jsp`.)
2. Log on with the Oracle SES admin user name `eqsys` and the password specified during installation.

22.6.4.2 Setting Up Oracle SES to Search Documents

To search WebCenter Portal documents using Oracle SES, you must first set up a Document Service Manager (with a Document Service Instance and a Document Service Pipeline), and then create a Content Server source.

1. Configure the Document Service Manager (one time for each Oracle SES instance).

Note: Document services are plug-ins involved in the processing of a document when it is being crawled. A document service allows WebCenter Portal to add indexable attributes for documents used in a WebCenter Portal application.

Search attribute names must be unique; two attributes cannot have the same name. For example, if an attribute exists with a String data type, and another attribute is discovered by the crawler with the same name but a different data type, then the crawler ignores the second attribute. Before creating new attributes, make sure to check the list of Oracle SES attribute names and types in the Oracle SES documentation.

- a. On the Global Settings - Document Services page, click **Create**. Select **Create New Manager**, click **Next**, and enter the following parameters:

Manager Class Name:

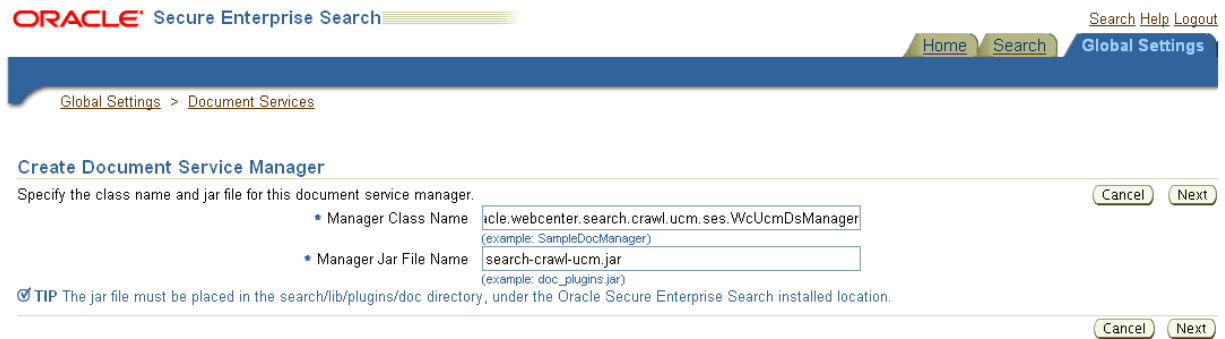
`oracle.webcenter.search.crawl.ucm.ses.WcUcmDsManager`

Manager Jar File Name: `search-crawl-ucm.jar`

Note: The `webcenter_search_ses_plugins.zip` file installs `Oracle_Home/search/lib/plugins/doc/search-crawl-ucm.jar`.

Click **Next**, and then click **Finish** ([Figure 22-29](#)).

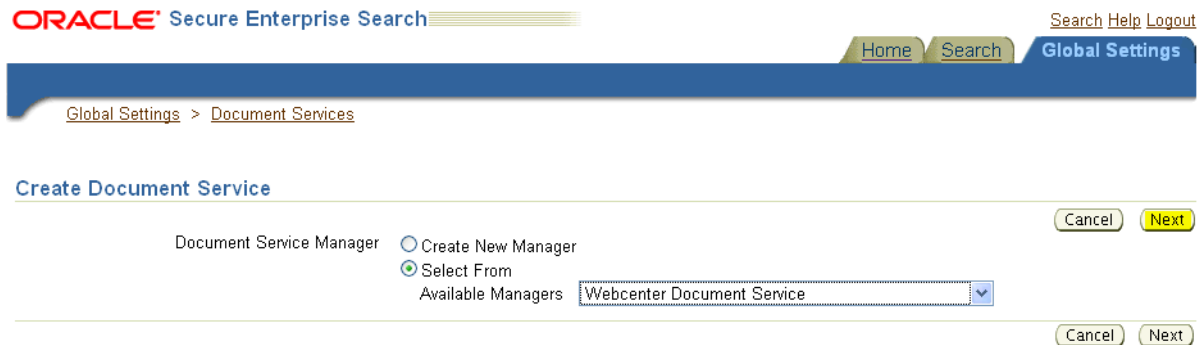
Figure 22–29 Creating a Document Services Manager in Oracle SES



b. Create the Document Service Instance.

Again, on the Global Settings - Document Services page, click **Create**. This time, select **Select From Available Managers with Secure Enterprise Search WebCenter UCM Plugin**, and click **Next** (Figure 22–30).

Figure 22–30 Create Document Service



In addition to the entering an instance name, enter the following parameters:

WebCenter Application Name: The unique name being used to identify this WebCenter Portal application in the back-end Content Server.

Connection Name: The name of the primary Content Server connection that WebCenter Portal is using to store Space documents.

WebCenter URL Prefix: The host and port where the WebCenter Portal application is deployed; for example: `http://myhost:8888`.

Note: Use the `listDocumentsSpacesProperties` command to determine the application name and connection name for Spaces, as described in Section 22.6.1, "Setting Up WebCenter Portal: Spaces for Oracle SES Search."

c. Create the Document Services Pipeline. This invokes the document service instance. Again, on the Global Settings - Document Services page, under the **Document Services Pipelines** section, click **Create**.

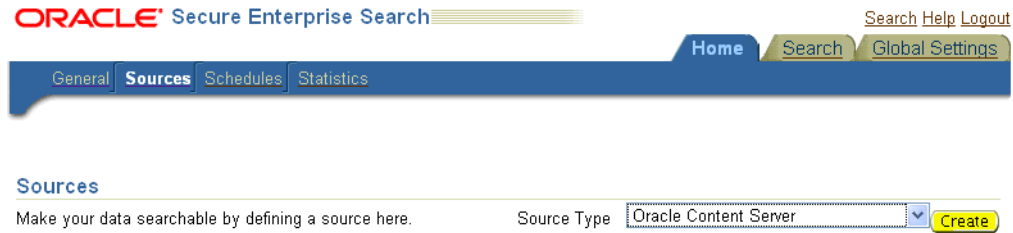
Enter a name and select the instance created in the previous step.

2. Create the Content Server source for documents.

See Also: [Section 22.6.5, "Configuring Search Crawlers Using WLST"](#) for an alternative way to create the Content Server source

- a. Go to **Home > Sources**.
- b. From the Source Type dropdown list, select **Oracle Content Server**, and click **Create** (Figure 22–31).

Figure 22–31 Create Oracle Content Server Source



- c. Enter the following parameters:

Source Name: *unique_name*

Configuration URL: *Content_Server_SES_Crawler_Export_endpoint*;
for example,

```
http://host:port/cs/idcplg?IdcService=SES_CRAWLER_DOWNLOAD_CONFIG&source=default
```

Note: The `source=default` parameter denotes the name of the source created in the configuration of the SES Crawler Export. The default one is created automatically and called "default."

Authentication Type:

If the Content Server is not protected by SSO, then enter `NATIVE`.

If the Content Server is protected by Oracle SSO, then enter `ORASSO`.

User ID: The user to crawl the Content Server must have the `sceCrawlerRole` role defined. The `sceCrawlerRole` is a configuration parameter in `SESCrawlerExport`. Typically, administrators create a special role, assign it no privileges to view content, then create a user account that has this role.

If you do not set up a specific `sceCrawlerRole`, then admin credentials are required to crawl. The `sysadmin` user ID works by default.

If Authentication Type is `ORASSO`, then enter a user ID (and password) of a user in the identity management server fronted by Oracle SSO. This user must have been granted the same permissions as `sysadmin`. If it is not possible to grant those permissions, then delete the "remote" user corresponding to this user in the Content Server, and create a "local" version of the user (same name) in the Content Server.

Password: Password for this Content Server user.

Realm:

If Authentication Type is NATIVE, then enter `Idc Security /cs/idcplg`, where `/cs/` is the context root you provided when you installing the Content Server.

If Authentication Type is ORASSO, then leave this parameter blank.

Scratch Directory: Optional. Specify a directory on the system under which the Oracle SES instance resides.

Oracle SSO Login URL:

If Authentication Type is ORASSO, then specify a value for Oracle SSO. For example:

`https://login.oracle.com/mysso/signon.jsp?site2pstoretoken`
=

If Authentication Type is NATIVE, then leave this field blank.

Oracle SSO Action URL:

If Authentication Type is ORASSO, then specify a value for Oracle SSO. For example: `https://login.oracle.com/sso/auth`

If Authentication Type is NATIVE, then leave this field blank.

Click **Next** (Figure 22–32).

Figure 22–32 Oracle Content Server Source Parameters

ORACLE Secure Enterprise Search Search Help Logout

Home Search Global Settings

General Sources Schedules Statistics

Home > Sources

Create User-Defined Source : Step 1 : Parameters Cancel Next

Source Name

Source Type **Oracle Content Server**

Name	Value	Description
Configuration URL	<code>rice=SES_CRAWLER_DOWNLOAD_CONFIG&source=default</code>	File/HTTP URL of the configuration file
Authentication Type	NATIVE	Standard Java authentication type used by the application serving the control and data feed. This parameter is relevant when the feeds are accessed over HTTP. Enter BASIC for basic authentication, FORM for form-based authentication, ORASSO for Oracle SSO, NATIVE for proprietary XML over HTTP authentication.
User ID	sysadmin	User ID for accessing feeds
Password	••••••••	Password for accessing feeds
Realm	<code>Idc Security /cs/idcplg</code>	Realm of the application serving the control and data feed. This parameter is relevant when the feeds are accessed over HTTP and is mandatory when the authentication type is BASIC.
Oracle SSO Login URL		Oracle SSO login URL protecting all SSO applications. This parameter is relevant when the authentication type is ORASSO.
Oracle SSO Action URL		Oracle SSO action URL authenticating SSO user credentials. This is the URL to which the SSO login form is submitted. This parameter is relevant when the authentication type is ORASSO.
Scratch Directory		Local directory where status files can be temporarily written
Maximum number of connection attempts	3	Maximum number of connection attempts to access data feed or upload status feed

- d. On the Create User-Defined Source : Step 2 : Authorization page, enter the following parameters in the Authorization Manager section, if not entered by default:

Plug-in Class Name:

`oracle.search.plugin.security.auth.stellent.StellentAuthManager`

Jar File Name: `oracleapplications/StellentCrawler.jar`

HTTP endpoint for authorization: for example,
`http://host:port/cs/idcplg`

Display URL Prefix: for example, `http://host:port/cs`

Authentication Type: NATIVE or ORASSO

Administrator User: The user to crawl the Content Server must have the `sceCrawlerRole` role defined. The `sceCrawlerRole` is a configuration parameter in `SESCrawlerExport`. Typically, administrators create a special role, assign it no privileges to view content, then create a user account that has this role.

If you do not set up a specific `sceCrawlerRole`, then admin credentials are required to crawl. The `sysadmin` user ID works by default.

If Authentication Type is ORASSO, then enter a user ID (and password) of a user in the identity management server fronted by Oracle SSO. This user must have been granted the same permissions as `sysadmin`. If it is not possible to grant those permissions, then delete the "remote" user corresponding to this user in the Content Server, and create a "local" version of the user (same name) in the Content Server.

Administrator Password: Password for crawl admin user

Authorization User ID Format: Authentication attribute used in the active identity plug-in. To find this value, go to the Global Settings - Identity Management Setup page in Oracle SES. Enter the value of the Authentication Attribute under the Active Plug-in (for example, `nickname` or `username` or something else). If you are using the Oracle E-Business Suite R12 identity plug-in, then leave the this parameter blank.

Realm:

If Authentication Type is NATIVE, then enter `Idc Security /cs/idcplg`, where `/cs/` is the context root you provided when you installing the Content Server.

In Authentication Type is ORASSO, then leave this field blank.

- e. Click **Create & Customize** (or edit a created source) to see other source parameters. On the **Crawling Parameters** tab, enter the following crawling parameter: `Document Service Pipeline`.
- f. Click **Enable** and select the pipeline you created.

22.6.4.3 Setting Up Oracle SES to Search Discussions and Announcements

To search WebCenter Portal discussions and announcements using Oracle SES, you must first set up two Oracle SES Database sources: one for discussions and one for announcements. For example, the discussions source could have the source name `GS_Discussions` and a View of `FORUMCRAWLER_VW`, and the announcements source might have the source name `GS_Announcements` and a View of `ANNOUNCEMENTS_VW`.

Note: There are slightly different steps for Oracle, Microsoft SQL Server, and IBM DB2 databases.

1. Configure the JDBC driver:
 - a. To crawl a Microsoft SQL Server or IBM DB2 database, download the appropriate JDBC driver jar files into the `ORACLE_HOME/search/lib/plugins/oracleapplications` directory in Oracle SES.

Note:

- For Microsoft SQL Server: Copy the Microsoft JDBC driver files `sqljdbc.jar` and `sqljdbc4.jar`.
 - DB2: Copy the IBM driver files `db2jcc.jar` and `db2jcc_license_cu.jar` (obtainable from the IBM DB2 UDB client).
-
-

If the JDBC drivers for JRE 1.5 and JRE 1.6 are different, (for example: `sqljdbc.jar` works for JRE 1.5 and `sqljdbc4.jar` works for JRE 1.6), then perform the following:

- Download both the driver jars into the `ORACLE_HOME/search/lib/plugins/oracleapplications` directory in Oracle SES.

- Add an entry for the JRE 1.6 version (`sqljdbc4.jar` for SQLServer) of the driver jar to the CLASSPATH element of `ORACLE_HOME/search/config/searchctl.conf`.

- Restart the middle tier.

- b. Update the `drivers.properties` file with the following information:
DatabaseName:DriverClassName.
- c. Add the JRE 1.5 JDBC driver jar file name to the classpath in `META-INF/MANIFEST.MF` of `appsjdbc.jar` and `DBCrawler.jar`.

For example, change:

```
Class-Path: sqljdbc.jar rsscrawler.jar ../../pluginmessages.jar
```

to

```
Class-Path: db2jcc.jar sqljdbc.jar rsscrawler.jar
../../pluginmessages.jar
```

and change:

```
Class-Path: appsjdbc.jar
```

to

```
Class-Path: db2jcc.jar appsjdbc.jar
```

For a key attribute that is not named `KEY`, change the JDBC driver information in the `drivers.properties` file to specify the key attribute name:

```
database_name: driver_class_name, key_attribute_name
```

For example, for a key attribute named ID:

```
oracle : oracle.jdbc.driver.OracleDriver, ID
```

In the crawling query, use *key_attribute_name* as the alias for the key value column name. In this example, ID is the alias for KEYVAL:

```
SELECT keyval id, content, url, lastmodifieddate, lang FROM sales_only
```

Oracle and SQL Server databases: The following default drivers are used if none is specified in `drivers.properties`:

- Oracle: `oracle.jdbc.driver.OracleDriver`
- SQL Server: `com.microsoft.sqlserver.jdbc.SQLServerDriver`

2. Required for IBM DB2 databases only:

- a. Make sure that no crawlers are running that use the database crawler source. In the Oracle SES administration tool, check the crawler progress and status on the Home - Schedules page. (Click **Refresh Status**.)
- b. Remake the `appsjdbc.jar` file and the `DBCrawler.jar` file. Ensure that the `META-INF/MANIFEST.MF` was updated correctly; otherwise, the crawler fails with the following error in the crawler log file:

```
EQP-80406: Loading JDBC driver failed
```

- c. Modify the

`Oracle_Home/search/lib/plugins/oracleapplications/drivers.properties` file to include the following line:

```
db2: com.ibm.db2.jcc.DB2Driver
```

- d. Include the driver jar (`db2jcc.jar`) to the `CLASSPATH` element of `ORACLE_HOME/search/config/searchctl.conf`. For example:

```
#CLASS PATH
CLASSPATH=ORACLE_HOME/search/webapp/config:ORACLE_HOME/search/webapp/
SESAuthenticator.jar:ORACLE_HOME/search/lib/plugins/commons-plugins-
stubs.jar :ORACLE_HOME /search/lib/plugins/oracleapplications/db2jcc.jar
```

- e. Edit `JVM_OPTIONS` in the

`ORACLE_HOME/search/config/searchctl.conf` file to add the system property `"-Doracle.home=ORACLE_HOME/search"`. For example:

```
JVM_OPTIONS= -Djava.awt.headless=true
-Dweblogic.RootDirectory=ORACLE_HOME/search/base_domain
-Doracle.home=ORACLE_HOME/search
```

- f. Copy the

`ORACLE_HOME/search/lib/plugins/oracleapplications/pluginmessages.jar` file to the `ORACLE_HOME/search/lib` directory.

- g. Create the database source. Make sure to enter the correct authorization query and confirm that the attribute name used in **Grant Security Attributes** matches the one used in the authorization query; otherwise, users do not get any results when searching for documents.

3. Create a Discussions source or an Announcements source.

See Also: [Section 22.6.5, "Configuring Search Crawlers Using WLST"](#) for an alternative way to create these sources

- a. In Oracle SES, go to **Home > Sources**.
- b. From the Source Type dropdown list, select **Database**, and click **Create** (Figure 22–33).

Figure 22–33 Create Database Source



- c. Enter the following parameters:

Source Name: *unique_name*; for example, *GS_Discussions* to crawl discussions (or *GS_Announcements* to crawl announcements)

Database Connection String: Enter one of the following

- Oracle database: Enter one of the following

`jdbc:oracle:thin:@host:port:sid`

`jdbc:oracle:thin@host:port/serviceId`

- IBM DB2 database: Enter `jdbc:db2://host:port/database_name`

- Microsoft SQL Server database: Enter

`jdbc:sqlserver://host_or_IP_address:port;database_name`

User ID: Enter one of the following

- Oracle database: The user *MyPrefix_DISCUSSIONS_CRAWLER* created during Oracle WebCenter Portal's Discussions Server installation

- Microsoft SQL Server database: The user *MyPrefix_DISCUSSIONS_CRAWLER* created during Oracle WebCenter Portal's Discussions Server installation

- IBM DB2 database: The user *MyPrefix_DC* created during Oracle WebCenter Portal's Discussions Server installation (where *MyPrefix* is five characters)

Password: Password for this user

Query: Enter one of the following queries:

`SELECT * FROM FORUMCRAWLER_VW`

`SELECT * FROM ANNOUNCECRAWLER_VW`

Use `FORUMCRAWLER_VW` for the source crawling discussion forums.

Use `ANNOUNCECRAWLER_VW` for the source crawling announcements.

URL Prefix: The URL prefix for the WebCenter Portal application, including host, port, and application name. For example,

`http://host:port/webcenter` for Webcenter Portal: Spaces.

Grant Security Attributes: `WCSECATTR`

Note: Previous releases of Content Server used FORUMID for **Grant Security Attributes**.

- d. Click **Next**.
- e. On the Create User-Defined Source : Step 2 : Authorization page, enter the following parameters (if not prepopulated) in the Authorization Manager section:

Plug-in Class Name:

oracle.search.plugin.security.auth.db.DBAuthManager

Jar File Name: oracleapplications/DBCrawler.jar

Authorization Database Connection String: Enter one of the following:

- Oracle database: Enter one of the following:

jdbc:oracle:thin:@host:port:sid

jdbc:oracle:thin@host:port/serviceId

- IBM DB2 database: Enter jdbc:db2://host:port/database_name

- Microsoft SQL Server database: Enter

jdbc:sqlserver://host_or_IP_address:port;database_name

User ID: Enter one of the following:

- Oracle database: Enter the user *MyPrefix_DISCUSSIONS_CRAWLER*

- Microsoft SQL Server database: Enter the user

MyPrefix_DISCUSSIONS_CRAWLER

- IBM DB2 database: Enter the user *MyPrefix_DC* (where *MyPrefix* is five characters)

Password: This user password

Single Record Query: false

Authorization Query: Enter the following (on one line):

```
SELECT DISTINCT forumID as WCSECATTR
FROM AUTHCRAWLER_FORUM_VW
WHERE username = ? UNION SELECT DISTINCT -1 as WCSECATTR
FROM AUTHCRAWLER_FORUM_VW
```

Note: Previous releases of Content Server used the following authorization query:

```
SELECT forumID
FROM AUTHCRAWLER_FORUM_VW
WHERE (username = ? or userID=-1)
UNION SELECT f.forumID
FROM jiveForum f, AUTHCRAWLER_CATEGORY_VW c
WHERE f.categoryID = c.categoryID AND (c.username = ? or
userID=-1)
```

Authorization User ID Format: Authentication attribute used in the active identity plug-in. To find this value, go to the Global Settings - Identity Management Setup page in Oracle SES. Enter the value of the Authentication

Attribute under the Active Plug-in (for example, nickname or username or something else).

If you are using the Oracle E-Business Suite R12 identity plug-in, then leave the this parameter blank.

- f. Click **Create** to complete the source creation.

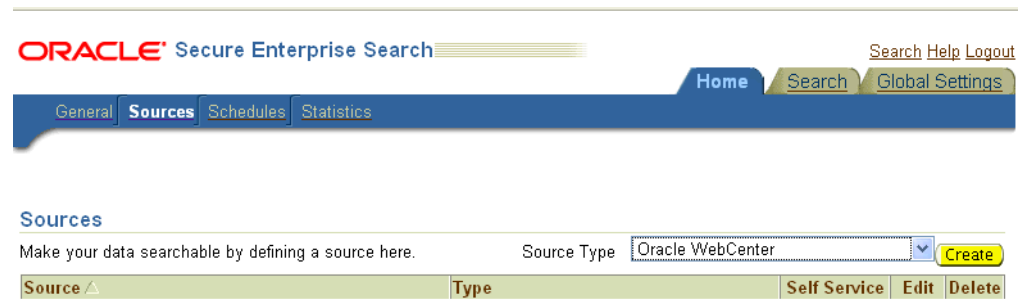
22.6.4.4 Setting Up Oracle SES to Search Spaces, Lists, Pages, and People

This section describes how to create the Oracle WebCenter source.

See Also: [Section 22.6.5, "Configuring Search Crawlers Using WLST"](#) for an alternative way to create the Oracle WebCenter source

1. Go to the **Home > Sources** page.
2. From the **Source Type** dropdown list, select the **Oracle WebCenter** source type, and click **Create** (Figure 22–34).

Figure 22–34 Create Oracle WebCenter Source



3. Enter the following source parameters:

Note: If WebCenter Portal is fronted with an Oracle HTTP Server, then the Configuration URL used in this step requires the following in `mod_wl_ohs.conf` file.

In a non-clustered environment:

```
<Location /rsscrawl>
SetHandler weblogic-handler
WebLogicHost host_name
WeblogicPort port
</Location>
```

```
<Location /sesUserAuth>
SetHandler weblogic-handler
WebLogicHost host_name
WeblogicPort port
</Location>
```

In a clustered environment:

```
<Location /rsscrawl>
WebLogicCluster host_name1:port,host_name2:port
SetHandler weblogic-handler
</Location>
```

```
<Location /sesUserAuth>
WebLogicCluster host_name1:port,host_name2:port
SetHandler weblogic-handler
</Location>
```

where *host_name1* and *host_name2* are the cluster nodes, and *port* is the listening port number of the managed server on which the WebCenter Portal application is deployed.

See Also: [Section 31.2.3.1, "Installing and Configuring OAM 11g"](#) for detailed information about using WebCenter Portal with Oracle Access Manager

Source Name: *unique_name*

Configuration URL: *host:port_of_WebCenterSpaces/rsscrawl*; for example, `http://myhost:8888/rsscrawl`

Authentication Type: BASIC

User ID: Crawl admin user you registered in [Section 22.3.2, "Oracle SES - Configuration"](#); for example, `mycrawladmin`

Password: Password for the crawl admin user

Realm: `jazn.com`

Oracle SSO Login URL: Leave this field blank.

Oracle SSO Action URL: Leave this field blank.

Scratch Directory: Optional. Specify a directory on the system under which the Oracle SES instance resides.

Number of connection attempts: Maximum number of connection attempts to access data feed or upload status feed.

Click [Next](#) (Figure 22–35).

Figure 22–35 Oracle WebCenter Source Parameters

ORACLE Secure Enterprise Search

Home Search Global Settings

General Sources Schedules Statistics

Home > Sources

Create User-Defined Source : Step 1 : Parameters

Source Name

Source Type **Oracle WebCenter**

Parameters

Name	Value	Description
Configuration URL	<input type="text" value="http://myhost:8888/rsscrawl"/>	File/HTTP URL of the configuration file
Authentication Type	<input type="text" value="BASIC"/>	Standard Java authentication type used by the application serving the control and data feed. This parameter is relevant when the feeds are accessed over HTTP. Enter BASIC for basic authentication, FORM for form-based authentication, ORASSO for Oracle SSO, NATIVE for proprietary XML over HTTP authentication.
User ID	<input type="text" value="mycrawladmin"/>	User ID for accessing feeds
Password	<input type="password" value="*****"/>	Password for accessing feeds
Realm	<input type="text" value="jazn.com"/>	Realm of the application serving the control and data feed. This parameter is relevant when the feeds are accessed over HTTP and is mandatory when the authentication type is BASIC.
Oracle SSO Login URL	<input type="text"/>	Oracle SSO login URL protecting all SSO applications. This parameter is relevant when the authentication type is ORASSO.
Oracle SSO Action URL	<input type="text"/>	Oracle SSO action URL authenticating SSO user credentials. This is the URL to which the SSO login form is submitted. This parameter is relevant when the authentication type is ORASSO.
Scratch Directory	<input type="text"/>	Local directory where status files can be temporarily written
Maximum number of connection attempts	<input type="text" value="3"/>	Maximum number of connection attempts to access data feed or upload status feed

- On the Create User-Defined Source : Step 2 : Authorization page, the Plug-in Class Name, Jar File Name, and Authorization Endpoint are prepopulated on the page.

Enter the following plug-in parameters:

Realm: `jazn.com`

User ID: Crawl admin user you registered [Section 22.3.2, "Oracle SES - Configuration"](#); for example, `mycrawladmin`

Password: Password for the crawl admin user

Authorization User ID Format: Authentication attribute used in the active identity plug-in. To find this value, go to the Global Settings - Identity Management Setup page in Oracle SES. Enter the value of the Authentication Attribute under the Active Plug-in (for example, `nickname` or `username` or something else). If you are using the Oracle E-Business Suite R12 identity plug-in, then leave the this parameter blank.

- Click **Create** to complete the source creation.

22.6.4.5 Excluding Services from the Spaces Crawler

The Spaces Crawler collects data for searching the following services:

- `oracle.webcenter.peopleconnections.profile` (People Connections)
- `oracle.webcenter.community` (Spaces)
- `oracle.webcenter.page` (Pages)
- `oracle.webcenter.list` (Lists)

Use the URL parameter `?excludedServiceIds` to disable search for any of these services. Add `?excludedServiceIds` after `/rsscrawl` when setting up the Oracle WebCenter source on Oracle SES. Set this parameter equal to the comma-delimited list of service IDs to exclude when crawling Spaces.

Example 22–10 Disable Crawling of People Connections

```
/rsscrawl?excludedServiceIds=oracle.webcenter.peopleconnections.profile
```

Example 22–11 Disable Crawling of Pages

```
/rsscrawl?excludedServiceIds=oracle.webcenter.page
```

Example 22–12 Disable Crawling of People Connections and Pages

```
/rsscrawl?excludedServiceIds=oracle.webcenter.peopleconnections.profile,oracle.webcenter.page
```

22.6.4.6 Additional Oracle SES Configuration

This section describes the required steps in the Oracle SES administration tool.

1. Create a *source group* that includes the names of the Content Server, Discussions, Announcements, and WebCenter Portal services sources you created.
 - a. Go to the Search - Source Groups page, and click **Create**.
 - b. Enter the same source group name entered in [Section 22.6.1, "Setting Up WebCenter Portal: Spaces for Oracle SES Search."](#)
 - c. From the **Select Source Type** dropdown list, select each source type (Database, Oracle Content Server, Oracle WebCenter), and then from the Available Sources listed for each source type, move the source you created for that source type into the Assigned Sources list.
 - d. Click **Finish**.
2. Optionally configure the security filter lifespan. This refreshes the authorization policies for users in the system. It is best to have a short lifespan when user policies change frequently. (This chapter uses Oracle Internet Directory identity plug-in as the example.)

For example, on the Global Settings - Query Configuration page, under **Secure Search Configuration**, enter 0 for **Security Filter Lifespan (minutes)**.

Valid values for the security filter lifespan are between 0 minutes (no cache) and 526500 minutes (cache for one year).

3. To index everything, you must force a full crawl for each source; that is, you must change the existing incremental crawl schedule for each source to first process ALL documents.

This step is very important, in that searching does not work unless the content is first indexed completely.

Note: You can set the schedule for the Spaces Crawler with the **fullCrawlIntervalInHours** parameter in WLST or the **Full Crawl Interval** parameter in Fusion Middleware Control.

Go to the Home - Schedules page, select the source schedule, and click **Edit** to force a full crawl.

After each source has been crawled, go back to the same page and change the crawl policy back to incremental (index documents that have changed since the previous crawl). Also, in the Frequency section of the page, select a non-manual type for running incremental crawl (for example, weekly or daily).

Note: Before the first crawl of the Content Server, remember to go to the Content Server Administration page, select **SES Crawler Export**, and take a snapshot. For more information, see [Section 22.6.2, "Setting Up Oracle WebCenter Portal: Content Server for Oracle SES Search."](#)

22.6.5 Configuring Search Crawlers Using WLST

You can use WLST commands to create crawlers and to start, stop and delete crawler schedules. These commands let you crawl new data in Oracle SES or delete old crawlers if the configuration data changes.

The following examples show some of these commands. For more information, see the section, "Search - Oracle SES Search Crawlers" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

Example 22–13 Create a Spaces Crawler in WLST

```
createSpacesCrawler(
'webcenter', 'webcenter_host', 'webcenter_port',
'http://ses-host:ses-port/search/api/admin/AdminService', 'ses-admin-pw',
'webcenter-crawl-user', 'webcenter-crawl-user-pw', '/tmp',
'authentication-id-format', 'ACCEPT_ALL', 'PROCESS_ALL', 'MANUAL', 1, 1,
'MONDAY', 1, 1, 1, 1)
```

where:

- *webcenter_host* = WebCenter Portal host name
- *webcenter_port* = WebCenter Portal port number
- *ses-host* = Oracle SES host name
- *ses-port* = Oracle SES port number
- *ses-admin-pw* = Oracle SES admin user password
- *webcenter-crawl-user* = WebCenter Portal crawl user name
- *webcenter-crawl-user-pw* = WebCenter Portal crawl user password
- *authentication-id-format* = Use 'nickname' if the Identity Management plug-in on Oracle SES is set to Oracle Internet Directory; otherwise, use the value of the **Authentication Attribute** parameter on the Identity Management plug-in on Oracle SES.

Example 22–14 Create a Documents Crawler in WLST

```
createDocumentsCrawler(
'portal', 'portal_host', 'portal_port',
'http://ses-host:ses-port/search/api/admin/AdminService', 'ses-admin-pw',
'http://ucm-host:ucm-port/cs/idcplg?IdcService=
SES_CRAWLER_DOWNLOAD_CONFIG&source=default', 'ucm-crawl-user',
'ucm-crawl-user-pw', '/tmp',
'http://ucm-host:ucm-port/cs/idcplg', 'http://ucm-host:ucm-port/cs',
'Idc Security /cs/idcplg', 'authentication-id-format', 'Document-pipeline',
'ACCEPT_ALL', 'PROCESS_CHANGED', 'MANUAL', 1, 1, 'MONDAY', 1, 1, 1, 1)
```

where:

- *portal* = Name of the WebCenter Portal application in which to perform this operation
- *portal_host* = Host name of the system where the application is running
- *portal_port* = Port number used to access the application
- *ses-host* = Oracle SES host name
- *ses-port* = Oracle SES port number
- *ses-admin-pw* = Oracle SES admin user password
- *ucm-host* = Content Server host name
- *ucm-port* = Content Server port number
- *ucm-crawl-user* = Content Server crawl user name
- *ucm-crawl-user-pw* = Content Server crawl user password
- *authentication-id-format* = Use 'nickname' if the Identity Management plug-in on Oracle SES is set to Oracle Internet Directory; otherwise, use the value of the **Authentication Attribute** parameter on the Identity Management plug-in on Oracle SES
- *Document-pipeline* = Document pipeline on Oracle SES created for this WebCenter Portal instance

Example 22-15 Create a Discussions Crawler in WLST

```
creatediscussionsCrawler(
'webcenter','webcenter_host','webcenter_port',
'http://ses-host:ses-port/search/api/admin/AdminService','ses-admin-pw',
'jdbc:oracle:thin:@database-host:database-port:database-sid',
'Jive-crawler-schema','Jive-crawler-schema-pw','authentication-id-format',
'ACCEPT_ALL','PROCESS_ALL','MANUAL',1,1,'MONDAY',1,1,1,1)
```

where:

- *webcenter_host* = WebCenter Portal host name
- *webcenter_port* = WebCenter Portal port number
- *ses-host* = Oracle SES host name
- *ses-port* = Oracle SES port number
- *ses-admin-pw* = Oracle SES admin user password
- *database-host* = Oracle WebCenter Portal's Discussion Server database host name
- *database-port* = Discussions server database port number
- *database-sid* = Discussions database name or SID
- *Jive-crawler-schema* = Discussions server crawler schema name. Determine the prefix from RCU, and use *rcu-prefix_DISCUSSION_CRAWLER*.
- *Jive-crawler-schema-pw* = Oracle WebCenter Portal's Discussions Server crawler schema password
- *authentication-id-format* = Use 'nickname' if the Identity Management plug-in on Oracle SES is set to Oracle Internet Directory; otherwise, use the value

of the **Authentication Attribute** parameter on the Identity Management plug-in on Oracle SES.

Note: To effect WLST changes, you must restart the managed server on which the application is deployed (by default, WC_Spaces). For more information, see the section "Starting and Stopping WebLogic Managed Servers Using the Command Line" in *Oracle Fusion Middleware Administrator's Guide*.

22.6.6 Configuring Oracle SES Search for Spaces Using Python Script

A sample Python script runs the steps done using WLST commands in [Section 22.6, "Configuring Oracle SES to Search Spaces Applications."](#) The sample script performs the following tasks:

- Create Federation Trusted Entity on Oracle SES
- Create crawl user with crawl role in WebCenter Portal
- Create connection to Oracle SES in WebCenter Portal
- Create WebCenter Portal crawl source in Oracle SES
- Create Content Server source in Oracle SES
- Create Discussions source and Announcements source in Oracle SES

Note: This script is supported only on Oracle SES 11.1.2 and above.

This sample script has the following prerequisites:

- [Section 22.6.2, "Setting Up Oracle WebCenter Portal: Content Server for Oracle SES Search"](#)
- [Section 22.6.3, "Setting Up Oracle WebCenter Portal Discussion Server for Oracle SES Search"](#)
- [Section 22.6.4, "Setting Up Oracle SES to Search WebCenter Portal"](#) (except for the steps to create crawl sources)

The sample Python script file and its properties file are in the `$WC_ORACLE_HOME/webcenter/scripts/ses_11.1.2/` directory.

Follow these steps to use the sample Python script:

1. Set an environment variable to reference the directory. For example:


```
setenv SESDIR Oracle_WC1/webcenter/scripts/ses_11.1.2/
```
2. Update the `ConfigureSES.properties` file with appropriate values.
3. Set default directory to the directory of `wlst.sh` script. For example:


```
cd Oracle_WC1/oracle/as11gr1wc/common/bin/
```
4. Run the `ConfigureSES.py` script with `ConfigureSES.properties`. For example:


```
./wlst.sh $SESDIR/ConfigureSES.py $SESDIR/ConfigureSES.properties
```
5. Restart WebCenter Portal after successful completion of the Python script.

22.6.7 Tips for Crawling Page Contents

To crawl page contents in a Framework application, follow these guidelines:

- In page templates, render pages as links using go links (`af:goLink`) instead of command links (`af:commandLink`).
- Disable iterative development in JDeveloper during crawling. Iterative development lets you make changes to your application while it is running and immediately see the effect of those changes by refreshing the page in your browser. The iterative development feature works by disabling certain optimization features.

Iterative development is enabled by default. To turn it off:

1. In JDeveloper, from the Application menu, select **Application Properties**.
2. Along the left side of the Application Properties dialog, expand the **Run** node.
3. Select **WebCenter Portal**.
4. Deselect **Enable Iterative Development**.
5. Click **OK**.

22.7 Troubleshooting Issues with Oracle SES Search

This section provides troubleshooting tips on administering Oracle SES search. It includes the following subsections:

- [Section 22.7.1, "No Search Results Found"](#)
- [Section 22.7.2, "Search Failure Errors"](#)
- [Section 22.7.3, "Cannot Grant View Permissions to WebCenter Portal"](#)
- [Section 22.7.4, "Restricting Oracle SES Results by Source Group or Source Type"](#)
- [Section 22.7.5, "Search Results Do Not Include Secured Resources"](#)
- [Section 22.7.6, "Search Results Do Not Include Documents"](#)
- [Section 22.7.7, "Search Results Do Not Include Discussions and Announcements"](#)
- [Section 22.7.8, "Search Results Do Not Include Recently Added Resources"](#)
- [Section 22.7.9, "Search Results Do Not Reflect Authorization Changes"](#)
- [Section 22.7.10, "Search Results Do Not Include Resources Available to Wide Audience"](#)

22.7.1 No Search Results Found

Problem

No search results are found.

Solution

Check the following:

- [Oracle SES Connection](#)
- [Documents and Discussions Connections](#)
- [WebCenter Portal Crawl Configuration](#)

- [Oracle SES Configuration](#)
- [User Authentication](#)
- [Oracle SES Crawling](#)
- [Oracle SES Authorization](#)

22.7.1.1 Oracle SES Connection

Confirm that you can access the Oracle SES SOAP URL and that connection properties to Oracle SES are correct.

For more information, see [Section 22.4.5, "Testing Oracle SES Connections."](#)

22.7.1.2 Documents and Discussions Connections

Confirm that connections exist in WebCenter Portal to the Content Server and the discussions server.

The Oracle SES search log shows if a WebCenter Portal service is excluded from the Oracle SES Search. Locate the search log file on the Oracle SES instance and check the log file for `totalSearchTime`.

No service excluded (that is, Oracle SES search is enabled for all WebCenter Portal services) looks similar to the following:

```
req=Search userName=vicki totalSearchTime=1150ms userQuery=0712>
```

Service excluded (that is, Oracle SES search is not enabled for Documents, Discussions, and Announcements) looks similar to the following:

```
req=Search userName=vicki totalSearchTime=1133ms userQuery=0712
-wc_serviceId:oracle.webcenter.doclib
-wc_serviceId:oracle.webcenter.collab.forum
-wc_serviceId:oracle.webcenter.collab.announcement>
```

22.7.1.3 WebCenter Portal Crawl Configuration

Use Fusion Middleware Control or WLST to confirm that Oracle SES search is enabled in WebCenter Portal, as described in [Section 22.6.1, "Setting Up WebCenter Portal: Spaces for Oracle SES Search."](#)

22.7.1.4 Oracle SES Configuration

1. Confirm that you have installed all required patches for Oracle SES. For the latest information on required patches, see "Back-End Requirements for the Search Service" in *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Portal* and the Release Notes.
2. Confirm that Oracle SES is configured with an identity management system to validate and authenticate users. Also confirm that WebCenter Portal and Oracle SES use the same identity management system, such as Oracle Internet Directory. All repositories you are using (such as WebCenter Portal: Spaces, WebCenter Portal Content: Content Server, and Oracle WebCenter Portal's Discussion Server) must share the same user base as Oracle SES.

Additionally, each Oracle SES instance must have a trusted entity for allowing WebCenter Portal end users to be securely propagated at search time. For more information, see [Section 22.3.2, "Oracle SES - Configuration."](#)

To test the Oracle SES is connection with a federated trusted entity user, see [Section 22.4.5, "Testing Oracle SES Connections."](#)

22.7.1.5 User Authentication

Confirm that the user exists (that is, confirm that the user can log on) in WebCenter Portal identity plug-ins, Oracle SES, and all configured data repositories, such as the Content Server and the discussions server.

An Oracle SES proxy login error in the WebCenter Portal diagnostic log looks similar to the following:

```
Received status "failed" during proxy login with application entity "weblogic" to
Oracle SES at [http://host:port/search/query/OracleSearch], as search user
"vicki". Defaulting to public.
```

22.7.1.6 Oracle SES Crawling

Confirm that Oracle SES crawled successfully in all sources.

1. In the Oracle SES administration tool, go to the Home - Schedules tab. Click the **Log File** icon to display the log file for the source. To obtain the location of the full log, click the **Status** link. The Crawler Progress Summary and Log Files by Source section displays the full path to the log file.
2. If Oracle SES fails to log in to the Content Server crawl endpoint due to an authentication error, then the following errors are logged:

```
EQP-60303: Exiting saxthread due to errors
```

```
EQP-80330: Unrecognized QName
<http://schemas.xmlsoap.org/soap/envelope/>:Envelope
oracle.search.sdk.crawler.PluginException
```

3. For the Oracle WebCenter source, verify if the rsscrawl servlet is unavailable. For example:

```
FATAL      main      EQP-80309: Exception while opening a stream to the
URI: https://example.com:port/rsscrawl?command=GetControl
```

4. For the Content Server source, verify if the password is invalid. For example:

```
XML error
```

5. Monitor the crawl process in the Oracle SES administration tool with a combination of the following:
 - a. Check the crawler progress and status on the Home - Schedules page. (Click Refresh Status.) From the Status page, you can view statistics of the crawl.
 - b. Monitor your crawler statistics on the Home - Schedules - Crawler Progress Summary page and the Home - Statistics page.
 - c. Monitor your search statistics on the Home - General page and the Home - Statistics page.

See *Oracle Secure Enterprise Search Administrator's Guide* for tips to tune crawl performance.

6. Additionally, examine snapshots and datafeeds on the Content Server instance, and examine the Oracle WebCenter Portal's Discussions Server database.

22.7.1.7 Oracle SES Authorization

1. In the Oracle SES administration tool, go to the Home - Sources tab.
2. Click the **Edit** icon for the source to see source configuration tabs.

3. Click the **Authorization** tab to confirm the authorization connection string, user name, password, and authorization user ID format.
4. Examine the Oracle SES log file (described in a previous step). Look for phrases including the URL value. For example:

```
ORA-01017: invalid username/password error
```

For detailed information on the Oracle SES administration tool, see the Oracle SES documentation included with the product. (This is listed in the WebCenter Portal product area on the Oracle Fusion Middleware documentation library.)

22.7.2 Search Failure Errors

Problem

The following search failure messages may appear inconsistently after a search:

```
Search failure: time out error
Search failure: problem preparing search executor
Search failure: problem with execution
```

Solution

Wait a moment, and try the search again. These messages appear when the service times out, which largely depends on the system load. If the time out error persists, adjust the `executionTimeout` parameter in the `setSearchConfig` command.

For command syntax and examples, see the section, "setSearchConfig" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

22.7.3 Cannot Grant View Permissions to WebCenter Portal

Problem

You get the following error when granting "view" permissions, as described in [Section 22.6.1, "Setting Up WebCenter Portal: Spaces for Oracle SES Search."](#)

```
Command FAILED, Reason: javax.naming.directory.AttributeInUseException: [LDAP: error code 20 - uniquemember attribute has duplicate value.]; remaining name 'orclguid=F0CC506017B711DFBFFED9EA6A94EAEC,cn=Permissions,cn=JAAS Policy,cn=webcenter,cn=wc_domain,cn=JPSCContext,cn=jpsroot_webcenter_dadvmc0057'
```

Solution

This error appears if the permission is granted. Ignore the error.

22.7.4 Restricting Oracle SES Results by Source Group or Source Type

Problem

You want to restrict search results by source group or source type.

Solution

In the Oracle SES admin tool, navigate to the Home - Sources - Customize Federated Source - Search Restrictions page to set search restrictions.

Alternatively, use filters, where each filter is a restriction on search result.

For detailed information about using Oracle SES, see the Oracle SES documentation on the Oracle Fusion Middleware documentation library (in the WebCenter Portal product area).

22.7.5 Search Results Do Not Include Secured Resources

Problem

Search results do not include secured resources. One cause is that the proxy login of WebCenter Portal users failed in Oracle SES. An Oracle SES proxy login error in the WebCenter Portal diagnostic log looks similar to the following:

```
Received status "failed" during proxy login with application entity "weblogic" to
Oracle SES at http://host:port/search/query/OracleSearch, as search user "vicki".
Defaulting to public.
```

Solution

Confirm that Oracle SES is configured with an identity management system to validate and authenticate users.

Also confirm that WebCenter Portal and Oracle SES use the same identity management system, such as Oracle Internet Directory. All repositories (such as WebCenter Portal: Spaces, WebCenter Portal Content: Content Server, and Oracle WebCenter Portal Discussions Server) must share the same user base as Oracle SES.

Additionally, each Oracle SES instance must have a trusted entity for allowing WebCenter Portal end users to be securely propagated at search time.

Problem

Search results do not include secured resources. Another cause is that authorization endpoints are not configured correctly. Locate the search log file on the Oracle SES instance. Look for phrases including the URL value. For example:

```
EQP-80309: Exception while opening a stream to the URI:
http://<host>:<port>/sesUserAuth?userId=<end-user-name>
```

```
QueryFilterPlugin returned null or empty array value for security attribute
"WCECATTR". Values required for all security attributes.
```

Solution

1. In the Oracle SES administration tool, go to the Home - Sources tab.
2. Click the **Edit** icon for the source to see source configuration tabs.
3. Click the Authorization tab to confirm the authorization connection string, user name, password, and authorization user ID format.

Problem

Search results do not include secured resources. Yet another cause is that authorization endpoints are not returning authorization data.

Locate the search log file on the Oracle SES instance. Look for phrases including the URL value. For example:

```
A security filter authorization timeout for dsid = # occurred after 10000
milliseconds.
```


Solution

Reduce the number of crawl sources.

22.7.6 Search Results Do Not Include Documents**Problem**

Search results do not include documents. Crawling of Content Server documents fails.

Solution

1. In the Oracle SES administration tool, go to the Home - Schedules tab.
2. Click the **Log File** icon to display the log file for the source. To obtain the location of the full log, click the **Status** link.
3. The Crawler Progress Summary and Log Files by Source section display the full path to the log file. If Oracle SES fails to log in to the Content Server crawl endpoint due to an authentication error, then the following errors are logged:

```
EQP-60303: Exiting saxthread due to errors,
EQP-80330: Unrecognized QName
<http://schemas.xmlsoap.org/soap/envelope/>:Envelope
oracle.search.sdk.crawler.PluginException
```

4. Update the configuration parameters of the Content Server crawl source.

22.7.7 Search Results Do Not Include Discussions and Announcements**Problem**

In the crawl source, the **Single Record Query** parameter is set to true on the Authorization tab.

Solution

Set the **Single Record Query** parameter to false.

Problem

The identity management system uses mixed case user name, but Oracle WebCenter Portal's Discussions Server (Jive) database uses all lowercase user name. The authorization query for the crawl source must apply the LOWER () function to user name parameters.

Solution

Confirm that the authorization query looks like the following statement:

```
SELECT forumID as WCSECATTR FROM AUTHCRAWLER_FORUM_VW WHERE LOWER(username) =
LOWER(?) UNION SELECT DISTINCT -1 as WCSECATTR FROM AUTHCRAWLER_FORUM_VW
```

22.7.8 Search Results Do Not Include Recently Added Resources**Problem**

A new resource was created recently, but search results do not include the new resource.

Solution

New resources must be crawled and indexed before they can be returned in search results. Crawl schedules are run periodically to index new content. If new resources are created often, then increase the frequency of the crawl schedule. If new resources need to be crawled immediately, then start that crawl schedule manually.

22.7.9 Search Results Do Not Reflect Authorization Changes

Problem

Some resources are accessible to more users due to authorization changes in WebCenter Portal. For example, resources in a space are now accessible to all authenticated users. The affected users cannot search for those resources.

Solution

Authorization data is cached in Oracle SES. The cache is invalidated according to the Security Filter Lifespan global setting in Oracle SES. The default value is 1 day or 1440 minutes. Adjust the value according to the general frequency of changes to authorization data.

22.7.10 Search Results Do Not Include Resources Available to Wide Audience

Problem

A WebCenter Portal space is publicly accessible, but unauthenticated users cannot see space resources in search results.

Solution

By default, view access of resources is granted to space members only, even if the space is accessible to the public. View access of resources must be granted to non-members explicitly. Go to the space settings page, select the Role tab and the intended role, and check view access to resources.

Managing the Worklist Service

This chapter describes how to configure and manage the Worklist service for WebCenter Portal applications (Spaces applications and Framework 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 Portal applications. Any changes that you make to Spaces applications and Framework applications, post deployment, are stored in MDS metadata store as customizations. See [Section 1.3.5, "WebCenter Portal Configuration Considerations."](#)

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

This chapter includes the following sections:

- [Section 23.1, "Configuration Roadmaps for the Worklist Service"](#)
- [Section 23.2, "What You Should Know About BPEL Connections"](#)
- [Section 23.3, "BPEL Server Prerequisites"](#)
- [Section 23.4, "Setting Up Worklist Connections"](#)
- [Section 23.5, "Troubleshooting Issues with Worklists"](#)

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."](#)

23.1 Configuration Roadmaps for the Worklist Service

Use the roadmaps in this section as an administrator's guide through the configuration process:

- [Section 23.1.1, "Roadmap - Configuring the Worklist Service for WebCenter Portal: Spaces"](#)

- Section 23.1.2, "Roadmap - Configuring the Worklist Service for Framework applications"

23.1.1 Roadmap - Configuring the Worklist Service for WebCenter Portal: Spaces

Figure 23–1 and Table 23–1 in this section provide an overview of the prerequisites and tasks required to get the Worklist service working in a Spaces application.

Figure 23–1 Configuring the Worklist Service for Spaces

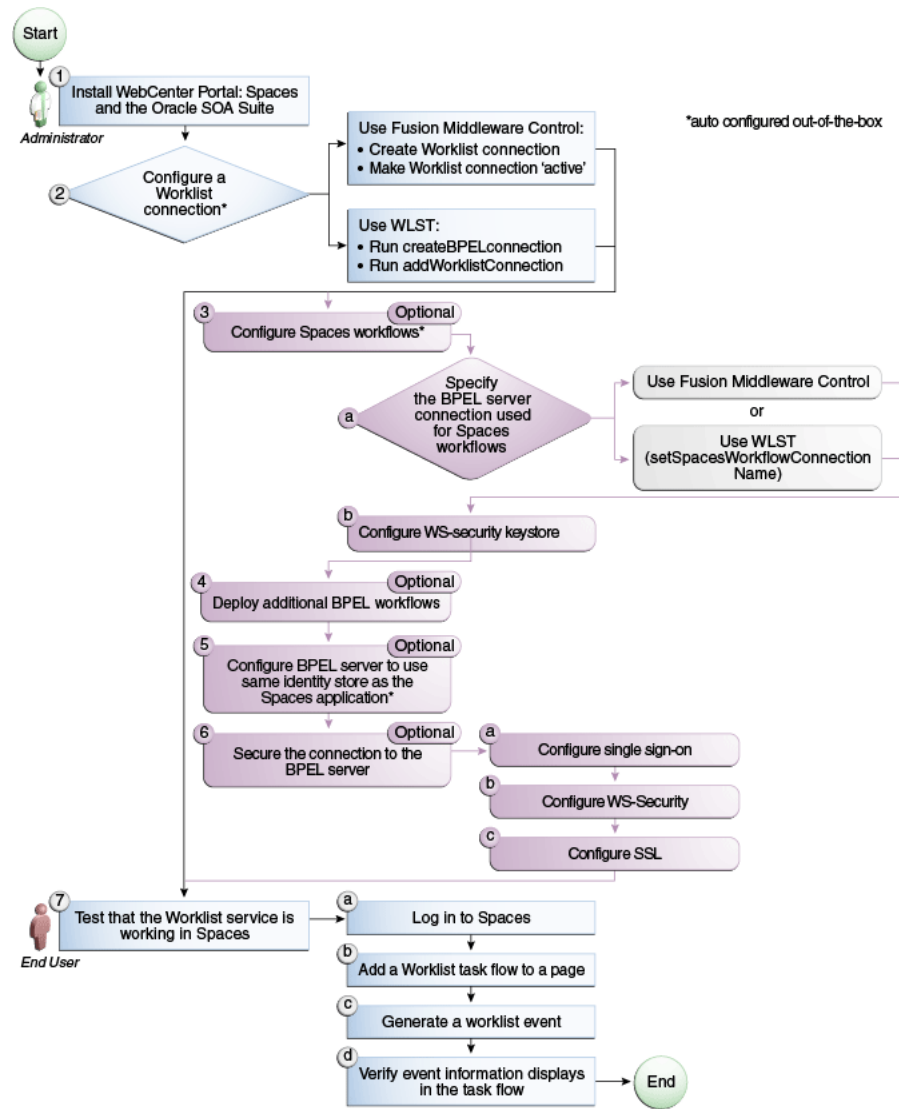


Table 23–1 Configuring the Worklist Service for Spaces

Actor	Task	Sub-Task
Administrator	1. Install WebCenter Portal: Spaces and the Oracle SOA Suite	

Table 23–1 (Cont.) Configuring the Worklist Service for Spaces

Actor	Task	Sub-Task
Administrator	2. Configure a Worklist connection using one of the following tools: ¹ <ul style="list-style-type: none"> ■ Use Fusion Middleware Control ■ WLST 	<p>When using Fusion Middleware Control:</p> <ul style="list-style-type: none"> ■ 2.a Create Worklist connection ■ 2.b Make Worklist connection 'active' <p>When using WLST:</p> <ul style="list-style-type: none"> ■ 2.a Run createBPELconnection ■ 2.b Run addWorklistConnection
Administrator	3. (Optional) Configure WebCenter Portal: Spaces workflows ¹	<p>3.a Specify the BPEL server connection used for WebCenter Portal: Spaces workflows using either of the following tools:</p> <ul style="list-style-type: none"> ■ Fusion Middleware Control ■ WLST (setSpacesWorkflowConnectionName) <p>3.b Configure WS-security keystore</p>
Administrator	4. (Optional) Deploy additional BPEL workflows	
Administrator	5. (Optional) Configure BPEL server to use same identity store as Spaces ¹	
Administrator	6. (Optional) Secure the connection to the BPEL server	<p>6.a Configure single sign-on</p> <p>6.b Configure WS-Security</p> <p>6.c Configure SSL</p>
End User	7. Test that the Worklist service is working in Spaces	<p>7.a Log in to Spaces</p> <p>7.b Add a Worklist task flow to a page</p> <p>7.c Generate a worklist event</p> <p>7.d Verify event information displays in the task flow</p>

¹ Auto configured out-of-the-box

23.1.2 Roadmap - Configuring the Worklist Service for Framework applications

Figure 23–2 and Table 23–2 in this section provide an overview of the prerequisites and tasks required to get the Worklist service working in Framework applications.

Figure 23–2 Configuring the Worklist Service for Framework applications

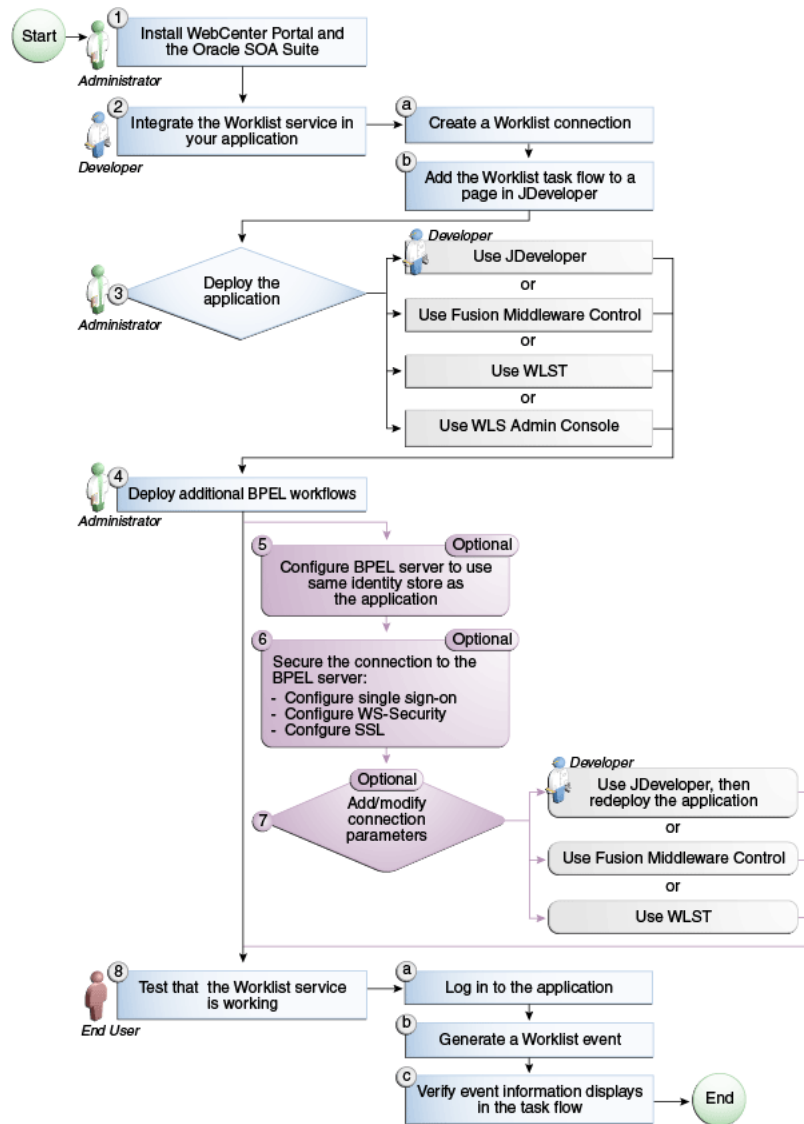


Table 23–2 Configuring the Worklist Service for Framework applications

Actor	Task	Sub-Task
Administrator	1. Install WebCenter Portal and the Oracle SOA Suite	
Developer	2. Integrate the Worklist service in your Framework application	2.a Create a Worklist connection 2.b Add the Worklist task flow to a page in JDeveloper

Table 23–2 (Cont.) Configuring the Worklist Service for Framework applications

Actor	Task	Sub-Task
Developer/Administrator	3. Deploy the Framework application using one of the following tools: <ul style="list-style-type: none"> ■ JDeveloper (Developer) ■ Fusion Middleware Control (Administrator) ■ WLST (Administrator) ■ WLS Admin Console (Administrator) 	
Administrator	4. Deploy additional BPEL workflows	
Administrator	5. (Optional): Configure BPEL server to use same identity store as the application	
Administrator	6. (Optional): Secure the connection to the BPEL server	6.a Configure single sign-on 6.b Configure WS-Security 6.c Configure SSL
Developer/Administrator	7. (Optional): Add/modify connection parameters using one of the following tools: <ul style="list-style-type: none"> ■ JDeveloper, then redeploy the application (Developer) ■ Fusion Middleware Control (Administrator) ■ WLST (Administrator) 	
End User	8. Test that the Worklist service is working	8.a Log in to the Framework application 8.b Generate a worklist event 8.c Verify event information displays in the task flow

23.2 What You Should Know About BPEL Connections

Consider the following while working with BPEL connections:

- The Worklist service allows multiple connections so that WebCenter Portal users can monitor and manage assignments and notifications from a range of BPEL servers. For more information, see [Section 23.4, "Setting Up Worklist Connections."](#)
- WebCenter Portal: Spaces workflows require a single connection to the BPEL server included with the Oracle SOA Suite. For more information, see [Section 9.3, "Specifying the BPEL Server Hosting Spaces Workflows."](#)
- The Worklist service and the WebCenter Portal: Spaces workflows can share the same BPEL server connection or each connect to different BPEL servers. To enable the display of worklist items created by the Spaces workflows in the current WebCenter Portal users' worklists, it is recommended that the WebCenter Portal: Spaces workflows and the Worklist service share a connection.
- The Worklist service can be wired to multiple BPEL connections to enable aggregation of worklist items from multiple BPEL servers. For example, when the

topology contains several BPEL servers running various workflow types, such as Human Resource and General Ledger servers.

- It is mandated that the BPEL connections are unique URLs. If this is not the case, then duplicate queries to the same server are created.

23.3 BPEL Server Prerequisites

Consider the following to ensure smooth functioning of the Worklists service:

- Pages that include Worklists task flows must be secured through ADF security.
- The Worklists service must be configured to use an Oracle SOA Suite BPEL server that is accessible through the BPEL Worklists application. The URL is in the following format:

```
http://host:port/integration/worklistapp
```

If the Worklist service is not running in the same domain as the Oracle SOA Suite BPEL server, the identity store (LDAP) should be either shared (recommended) or contain identical user names.

- Clocks on the Worklists service's managed server and the Oracle SOA Suite BPEL's managed server must be synchronized such that the SAML authentication condition, `NotBefore`, which checks the freshness of the assertion, is not breached.
- No configuration-related exceptions must exist. Use the WLST command `listWorklistConnections` to display the configured connections and validate the connection details. After listing the connections, validate them using the URL property appended with `/integration/worklistapp`. Hence, verify that `http://host:port/integration/worklistapp` can access the BPEL Worklist application.
- If the Oracle SOA Suite BPEL's managed server is configured to use an identity store and that store does not contain `BPMWorkflowAdmin`, `weblogic` by default, then the `BPMWorkflowAdmin` user must be configured, as described in [Section 23.5.2.2, "Shared User Directory Does Not Include the weblogic User."](#)
- The `wsm-pm` application 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 BPEL server issues, see [Section 23.5, "Troubleshooting Issues with Worklists."](#)

This section includes the following subsections:

- [Section 23.3.1, "BPEL Server - Installation and Configuration"](#)
- [Section 23.3.2, "BPEL Server - Security Considerations"](#)
- [Section 23.3.3, "BPEL Server - Limitations in WebCenter Portal"](#)

23.3.1 BPEL Server - Installation and Configuration

The Worklist service relies on the Oracle BPEL Process Manager (BPEL) server, which is included with Oracle SOA Suite.

To work with the Worklist service, you must install Oracle SOA Suite. For information about how to install Oracle SOA Suite, see the *Oracle Fusion Middleware Installation Guide for Oracle SOA Suite and Oracle Business Process Management Suite*.

After installing Oracle SOA Suite, you can integrate the Worklist service into your WebCenter Portal application by setting up connections to the BPEL server.

23.3.2 BPEL Server - Security Considerations

The Worklist service displays tasks for the currently authenticated user. For WebCenter Portal users to store and retrieve tasks on an Oracle SOA Suite BPEL server, their user names must either exist in a shared user directory (LDAP), or be set up similarly on both the WebCenter Portal application and the BPEL Server.

For example, if the user `rsmith` wants to use the Worklist service to store and retrieve tasks from the BPEL server, you must ensure that the user `rsmith` exists on both the BPEL server and within your application.

To access BPEL task details from the WebCenter Portal Worklist component, without incurring additional login prompts, WebCenter Portal and Oracle SOA Suite servers must be configured to a shared Oracle Single Sign-On server. For more information, see [Section 31.2, "Configuring Oracle Access Manager \(OAM\)"](#) and [Section 31.3, "Configuring Oracle Single Sign-On \(OSSO\)."](#)

For a secure connection you can optionally configure WS-Security between SOA and Spaces. For information, see [Chapter 34, "Configuring WS-Security."](#)

23.3.3 BPEL Server - Limitations in WebCenter Portal

Worklist task flows function inside authenticated pages only. If Worklist task flows are placed on unsecured pages, that is public pages that are not navigated to from an application on which the user has logged in, the warning message "You must log in to view Worklist content." is displayed. This is done to ensure that a session for the current users is available to determine which user's tasks are to be queried.

23.4 Setting Up Worklist Connections

This section includes the following subsections:

- [Section 23.4.1, "What You Should Know About Worklist Connections"](#)
- [Section 23.4.2, "Registering Worklist Connections"](#)
- [Section 23.4.3, "Activating a Worklist Connection"](#)
- [Section 23.4.4, "Modifying Worklist Connection Details"](#)
- [Section 23.4.5, "Deleting Worklist Connections"](#)

23.4.1 What You Should Know About Worklist Connections

The Worklist service enables WebCenter Portal applications to show authenticated users a list of BPEL worklist items currently assigned to them. BPEL worklist items are open BPEL tasks from one or more BPEL worklist repositories.

A connection to every BPEL server that delivers worklist items is required. Multiple worklist connections are allowed so that WebCenter Portal users can monitor and manage assignments and notifications from a range of BPEL servers.

If a BPEL server cannot be contacted, the Worklist task flow indicates that the connection is unavailable and any reason for the error is recorded in the server's diagnostic log. This log is located on the server that hosts the worklist component's log directory. For a Spaces application:

```
./user_projects/domains/base_domain/servers/WC_Spaces/logs/WC_Spaces-diagnostic.log.
```

For a Framework application:

```
./user_projects/domains/base_domain/servers/WC_Spaces/logs/WC_Cu  
stomPortal-diagnostic.log.
```

WebCenter Portal: Spaces

Spaces requires a BPEL server connection to support its internal workflows, that is, space membership notifications and space subscription requests. The BPEL server providing this functionality is always a BPEL server included with the Oracle SOA Suite. For more information, see [Section 9.3, "Specifying the BPEL Server Hosting Spaces Workflows."](#)

The Worklist service can share the SOA instance connection and by doing so, display worklist items relating to space activity in each user's Worklist task flow.

23.4.2 Registering Worklist Connections

This section includes the following subsections:




- [Section 23.4.2.1, "Registering Worklist Connections Using Fusion Middleware Control"](#)
- [Section 23.4.2.2, "Registering Worklist Connections Using WLST"](#)

23.4.2.1 Registering Worklist Connections Using Fusion Middleware Control

To register a Worklist connection:

1. Log in to Fusion Middleware Control and navigate to the home page for Spaces or the Framework application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
3. From the list of services on the **WebCenter Portal Service Configuration** page, select **Worklist**.
4. To register a new connection, click **Add** ([Figure 23-3](#)).

Figure 23–3 Configuring Worklist Connections

Manage Worklist Connections		
 Add  Edit  Delete		
Name	BPEL SOAP URL	Active Connection
WebCenter Worklist	http://hostname:portnumber	✓

5. Enter a unique name for the Worklist connection and set it as the active connection (Table 23–3). This connection is picked up after you restart the managed server.

Table 23–3 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 Portal application.</p> <p>This name may be displayed to users working with the worklist feature in the 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>
Active Connection	<p>Select to activate this worklist connection in the WebCenter Portal 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 Portal 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"> ■ Worklist Indicates whether the Worklist service displays items associated with this connection. ■ WebCenter Portal: Spaces Indicates whether Spaces uses the same BPEL server connection for internal workflows, such as space membership notifications, space subscription requests, and more. The BPEL server that provides this functionality is the BPEL server included with the Oracle SOA Suite. For more information, see Section 9.3, "Specifying the BPEL Server Hosting Spaces Workflows." <p>Although not shown here, the Notification service might be set up to use the BPEL server connection too. See, Section 19.2, "Setting Up Notifications".</p> <p>Before modifying connection properties, consider impact to any other components that share this connection.</p>

6. Enter connection details for the BPEL server (Table 23–4).

Table 23–4 Worklist Connection - Connection Details

Field	Description
BPEL Soap URL	<p>Enter the URL required to access the BPEL server. Use the format:</p> <p><i>protocol://host:port</i></p> <p>For example: <code>http://mybpelserver.com:8001</code></p> <p>Note: Spaces uses the BPEL server included with the Oracle SOA Suite to implement WebCenter Portal: Spaces workflows. If you are setting up the workflow connection, make sure you enter the SOA Suite's BPEL server URL here. For more information, see Section 9.3, "Specifying the BPEL Server Hosting Spaces Workflows."</p>
SAML Token Policy URI	<p>Select the SAML (Security Assertion Markup Language) token policy this connection uses for authentication.</p> <p>SAML is an XML-based standard for passing security tokens defining authentication and authorization rights. An attesting entity (that has a trusted 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"> ■ SAML Token Client Policy (<code>oracle/wss10_saml_token_client_policy</code>) - Select to verify your basic configuration without any additional security. This is the default setting. ■ SAML Token With Message Protection Client Policy (<code>oracle/wss10_saml_token_with_message_protection_client_policy</code>) - Select to increase the security using SAML-based BPEL Web Services. If selected, you must configure keys stores both in your WebCenter Portal application and in the BPEL application. For information, see Chapter 34, "Configuring WS-Security."
Recipient Key Alias	<p>The recipient key alias to be used for message protected SAML policy authentication. Only required when the BPEL server connection is using a SAML token policy for authentication and the application's Worklist service is using multiple BPEL server connections.</p> <p>For example, <code>myKey</code></p> <p>To determine the recipient key alias for a complex topology, see Section 34.3, "Configuring WS-Security for a Complex Topology."</p>
Link URL	<p>Specify the URL used to link to the BPEL server. Only required if it is different to the BPEL SOAP URL, for example, when SSO or HTTPS is configured.</p> <p>Use the format: <i>protocol://host:port</i></p> <p>For example, <code>http://mySSO.host.com:7777</code></p> <p>For performance reasons, in an HTTPS or SSO environment, the Link URL specifies user access to BPEL worklist items, through HTTPS or SSO Web servers, whereas the BPEL SOAP URL specifies direct access to BPEL Web services, without redirection through HTTPS or SSO Web servers.</p>

7. Click **OK** to save this connection.
8. Click **Test** to verify if the connection you created works. For a successful connection, the Test Status message displays the advice that to start using the new

(active) connection, you must restart the managed server on which the WebCenter Portal application is deployed. For more information, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

See [Section 23.5, "Troubleshooting Issues with Worklists"](#) if the test fails.

Tip: To activate newly registered connections, perform the steps described in [Section 23.4.3, "Activating a Worklist Connection."](#)

23.4.2.2 Registering Worklist Connections Using WLST

Use the WLST command `createBPELConnection` to create a BPEL server connection. For command syntax and examples, see the section, "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. For more information, see [Section 23.4.3.2, "Activating a Worklist Connections Using WLST."](#)

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

Note: To activate newly registered connections, perform the steps described in [Section 23.4.3, "Activating a Worklist Connection."](#)

To start using the new (active) connection you must restart the managed server on which the WebCenter Portal application is deployed. For more information, see the section, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

23.4.3 Activating a Worklist Connection

In WebCenter Portal applications, multiple Worklist connections may be active at a time. Multiple connections enable WebCenter Portal 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 so no errors or warnings are logged or displayed in the UI if the Worklist service queries a SOA server which is undergoing maintenance.

This section includes the following subsections:

- [Section 23.4.3.1, "Activating a Worklist Connections Using Fusion Middleware Control"](#)
- [Section 23.4.3.2, "Activating a Worklist Connections Using WLST"](#)

23.4.3.1 Activating a Worklist Connections Using Fusion Middleware Control

To activate or disable a Worklist connection:

1. Log in to Fusion Middleware Control and navigate to the home page for Spaces or the Framework application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:

- For the Spaces application - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
3. From the list of services on the **WebCenter Portal Services Configuration** page, select **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 Portal 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. Click **Test** to verify if the connection you activated works. For a successfully activated connection, the Test Status message displays the advice that to start using the updated connection, you must restart the managed server on which the WebCenter Portal application is deployed. For more information, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

23.4.3.2 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 the section, "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" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

Use `listWorklistConnections` to see which connections are currently active.

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

Note: To start using the active connection you must restart the managed server on which the WebCenter Portal application is deployed. For more information, see the section, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

23.4.4 Modifying Worklist Connection Details

This section includes the following subsections:

- [Section 23.4.4.1, "Modifying Worklist Connection Details Using Fusion Middleware Control"](#)

- [Section 23.4.4.2, "Modifying Worklist Connection Details Using WLST"](#)

23.4.4.1 Modifying Worklist Connection Details Using Fusion Middleware Control

To update worklist connection details:

1. Log in to Fusion Middleware Control and navigate to the home page for Spaces or the Framework application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:
 - For the Spaces application- From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
3. From the list of services on the **WebCenter Portal Services Configuration** page, select **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 23–4, "Worklist Connection - Connection Details"](#).
6. Click **OK** to update the connection.
7. Click **Test** to verify if the updated connection works. For a successfully updated connection, the Test Status message displays the advice that to start using the updated connection, you must restart the managed server on which the WebCenter Portal application is deployed. For more information, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

23.4.4.2 Modifying Worklist Connection Details Using WLST

Use the WLST command `setBPELConnection` to edit existing BPEL server connection details. For command syntax and examples, see the section, "setBPELConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.13.3.1, "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 Portal application is deployed. For more information, see the section, "Starting and Stopping WebLogic Managed Servers Using the Command Line" in the *Oracle Fusion Middleware Administrator's Guide*.

23.4.5 Deleting Worklist Connections

Several WebCenter Portal components can share the same worklist connection, that is, the Worklist service, Notifications service, and, Spaces workflows. Before you delete a Worklist connection, navigate to the Application Configuration page in Fusion Middleware Control (WebCenter Portal > Settings > Application Configuration) to verify whether Spaces Workflows and Notifications are using the connection.

This section includes the following subsections:

- [Section 23.4.5.1, "Deleting Worklist Connections Using Fusion Middleware Control"](#)
- [Section 23.4.5.2, "Deleting Worklist Connections Using WLST"](#)

23.4.5.1 Deleting Worklist Connections Using Fusion Middleware Control

To delete a worklist connection:

1. Log in to Fusion Middleware Control and navigate to the home page for Spaces or the Framework application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
3. From the list of services on the **WebCenter Portal Services Configuration** page, select **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 Portal application is deployed. For more information, see [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

23.4.5.2 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 the section, "deleteConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

Use the WLST command `removeWorklistConnection` to remove a BPEL server that is configured in `adf-config.xml`. The Worklist service no longer uses the connection specified but BPEL server connection details are retained in `connections.xml` for future use.

Use the WLST command `deleteConnection` to remove a BPEL server connection from `connections.xml`.

For command syntax and detailed examples, see "removeWorklistConnection" and "deleteConnection" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

Restart the managed server so that changes can take place.

23.5 Troubleshooting Issues with Worklists

The Worklist service relies on several middleware components to display worklist items to logged-in users and therefore, several factors may cause the Worklist service to fail. The issues and solutions discussed in this section relate to some common problems you may encounter.

This section includes the following subsections:

- [Section 23.5.1, "Unavailability of the Worklist Service Due to Application Configuration Issues"](#)
- [Section 23.5.2, "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.

23.5.1 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 subsections:

- [Section 23.5.1.1, "adf-config.xml Refers to a Non-Existent BPEL Connection"](#)
- [Section 23.5.1.2, "adf-config.xml Has No Reference to a BPEL Connection"](#)
- [Section 23.5.1.3, "No Rows Yet Message Displays"](#)

23.5.1.1 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 23.4, "Setting Up Worklist Connections."](#)

During development, see the chapter "Integrating the Worklist Service" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

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*.

23.5.1.2 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:
0000I0mqx8Fk3FLN2o2ye191qBV000008,0] [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 23.4.2, "Registering Worklist Connections."](#) 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 Portal*. Do not modify `adf-config.xml` and `connections.xml` files manually.

23.5.1.3 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 Portal*.

23.5.2 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 the Oracle SOA Suite BPEL processes run. 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 that is used for WS security. There can also be some other causes related to the exception. It is recommended that you examine the logged exceptions on both the WebCenter managed server and the configured Oracle SOA suites managed servers when these issues occur.

This section includes the following sub sections:

- [Section 23.5.2.1, "Users Mismatch in Identity Stores"](#)
- [Section 23.5.2.2, "Shared User Directory Does Not Include the weblogic User"](#)
- [Section 23.5.2.3, "Issues with the wsm-pm Application"](#)
- [Section 23.5.2.4, "Clocks are Out of Sync for More Than Five Minutes"](#)
- [Section 23.5.2.5, "Worklist Service Timed Out or is Disabled"](#)

23.5.2.1 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 Portal*.

This can be easily accomplished with a common LDAP identity store. A useful check is to validate that you can log in to 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.

23.5.2.2 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 `SOA_ORACLE_HOME`. For example:

```
cd $SOA_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.

23.5.2.3 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 the `wsm-pm` application, log in to 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.

23.5.2.4 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.

23.5.2.5 Worklist Service Timed Out or is Disabled

Problem

The Worklist service cannot obtain a query result from the Oracle SOA Suite BPEL server within a defined period.

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 quickly. In such a case, the logs contain

```
oracle.webcenter.concurrent.DisabledException
exceptions. These exceptions are related to the Worklist service failure.
```

Managing Portlet Producers

This chapter describes how to register, edit, delete, and deploy WSRP and Oracle PDK-Java portlet producers.

Note: Pagelet producer registration is described in a different chapter. For details, see [Section 25.2, "Registering the Pagelet Producer"](#).

System administrators can use Fusion Middleware Control or the WLST command-line tool to register and manage WSRP and Oracle PDK-Java portlet producers for WebCenter Portal application deployments.

Application administrators can also register and manage portlet producers at runtime through out-of-the-box administration pages or using the portlet producer task flow.

This chapter includes the following sections:

- [Section 24.1, "What You Should Know About Portlet Producers"](#)
- [Section 24.2, "Registering WSRP Producers"](#)
- [Section 24.3, "Testing WSRP Producer Connections"](#)
- [Section 24.4, "Registering Oracle PDK-Java Producers"](#)
- [Section 24.5, "Testing Oracle PDK-Java Producer Connections"](#)
- [Section 24.6, "Editing Producer Registration Details"](#)
- [Section 24.7, "Deregistering Producers"](#)
- [Section 24.8, "Deploying Portlet Producer Applications"](#)
- [Section 24.9, "Configuring WebCenter Services Portlets"](#)
- [Section 24.10, "Troubleshooting Portlet Producer Issues"](#)

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). For more information, see [Section 1.13, "Oracle WebCenter Portal Administration Tools."](#)

24.1 What You Should Know About Portlet Producers

Consider the following while working with portlet producers:

- Several out-of-the-box producers are provided with WebCenter Portal: OmniPortlet, Web Clipping, and WSRP Tools. The following EAR files are packaged with WebCenter Portal:
 - `portalTools.ear` - OmniPortlet and Web Clipping
 - `wsrp-tools.ear` - WSRP Tools
- You can install the `portalTools.ear` and `wsrp-tools.ear` files using the `registerOOTBProducers` WLST command. For command syntax and examples, see "registerOOTBProducers" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.
- Before users can add JSR 286 or Oracle PDK-Java portlets to a page, you must register the owning WSRP and Oracle PDK-Java producers. 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 installed, see the section "Extending an Existing Domain" in the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Portal* to install it in the production environment.
 - When you create a connection to a portlet producer, the producer is registered with the WebCenter Portal application and the connection is added to the `connections.xml` file. 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, connection metadata is created in the Oracle Metadata Services (MDS) repository and in the producer being registered. When a producer is consumed, the user customizations are saved to the producer. During deregistration the producer connection and customizations are removed.
 - All post deployment connection configuration is stored in MDS. For more information, see [Section 1.3.5, "WebCenter Portal 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 in the WebCenter Portal application; it is not necessary to restart the WebCenter Portal 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 Portal*.
 - For information on securing portlet producers, see [Section 35.1, "Securing a WSRP Producer"](#) and [Section 35.2, "Securing a PDK-Java Producer."](#)

24.2 Registering WSRP Producers

This section describes how to register WSRP producers for a deployed application, using Fusion Middleware Control and WLST commands. This section includes the following subsections:

- [Section 24.2.1, "Registering a WSRP Producer Using Fusion Middleware Control"](#)
- [Section 24.2.2, "Registering a WSRP Producer Using WLST"](#)

- [Section 24.2.3, "Adding a Grant to the Policy Store for a Mapped User Identity"](#)
- [Section 24.2.4, "Registering a WSRP Portlet Producer in WebCenter Portal: Spaces"](#)
- [Section 24.2.5, "Registering a WSRP Portlet Producer in WebCenter Portal: Framework Applications"](#)

For information about how to register WSRP producers at design-time, using JDeveloper, see the section "How to Register a WSRP Portlet Producer" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

24.2.1 Registering a WSRP Producer Using Fusion Middleware Control

To register a WSRP portlet producer:

1. Log in to Fusion Middleware Control and navigate to the home page for the WebCenter Portal application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#).
2. Do one of the following:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
3. In the **Add Portlet Producer Connection** section, enter connection details for the WSRP producer.

For detailed parameter information, see [Table 24–1](#).

Table 24–1 WSRP Producer Connection Parameters

Field	Description
Connection Name	Enter a unique name to identify this portlet producer registration within the WebCenter Portal application. The name must be unique across all WebCenter Portal connection types. The name you specify here appears in Composer (under the <i>Portlets</i> folder).
Producer Type	Indicate the type of this producer. Select WSRP Producer .

Table 24–1 (Cont.) WSRP Producer Connection Parameters

Field	Description
WSDL URL	<p>The registration URL for the WSRP producer.</p> <p>The syntax varies 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"> ■ host_name is the server where your producer is deployed. ■ port_number is the HTTP listener port number. ■ context_root is the Web application's context root. ■ portlets_wsrp(1 2)?WSDL is static text. All producers deployed to the Oracle WSRP container are exposed as WSRP version 1 and version 2 producers. <p>In WebCenter Portal: 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 WSRP producers, you can obtain this registration URL 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 Portal application must use an HTTP proxy when contacting this producer. If selected, enter values for Proxy Host and Proxy Port.</p> <p>A proxy is required when the WebCenter Portal 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 host name or IP address of 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. The default port is 80.</p>
Default Execution Timeout (Seconds)	<p>Enter a suitable timeout for communications with the producer, in seconds. For example, the maximum time the producer may take to register, deregister, or display portlets on WebCenter Portal application pages. The default is 30 seconds.</p> <p>Individual portlets may define their own timeout period, which takes precedence over the value expressed here.</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 Portal application. WebCenter Portal applications support six types of security tokens: *WSS 1.0 Username Token Without*

Password, WSS 1.0 Username Token With Password, WSS 1.0 SAML Token, WSS 1.0 SAML Token With Message Integrity, WSS 1.0 SAML Token With Message Protection, and WSS 1.1 SAML Token With Message Protection.

Where SAML is an abbreviation for Security Assertion Markup Language.

Note: PeopleSoft WSRP producers support two profiles: *Username Token With Password* and *SAML Token With Message Integrity*. Oracle Portal (as a consumer) supports three profiles: *Username Token Without Password, Username Token With Password, SAML Token With Message Integrity*. Other Oracle WSRP producers support all six profiles. For other WSRP containers, check with the specific vendor to determine the token formats they support.

For detailed parameter information, see [Table 24-2](#).

Table 24-2 WSRP Producer Security Connection Parameters

Field	Description
Token Profile	<p>Select the type of token profile to use for authentication with this WSRP producer. Select from:</p> <ul style="list-style-type: none"> <p>■ WSS 1.0 SAML Token With Message Integrity (wss10_saml_token_with_message_integrity_client_policy)—This policy provides message-level integrity protection and SAML-based authentication for outbound SOAP requests in accordance with the WS-Security 1.0 standard. A SAML token, included in the SOAP message, is used in SAML-based authentication with sender vouches confirmation. This policy uses WS-Security's Basic 128 suite of asymmetric key technologies and SHA-1 hashing algorithm for message integrity.</p> <p>■ WSS 1.0 SAML Token With Message Protection (oracle/wss10_saml_token_with_message_protection_client_policy)—This policy provides message-level protection (integrity and confidentiality) and SAML-based authentication for outbound SOAP requests in accordance with the WS-Security 1.0 standard. The web service consumer includes a SAML token in the SOAP header and the confirmation type is sender-vouches. This policy 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>■ WSS 1.0 Username Token Without Password (oracle/wss10_username_id_propagation_with_msg_protection_client_policy)—This policy provides username (with password) token profile based identity propagation with certificate based message protection for outbound SOAP requests in accordance with the WS-Security 1.0 standard. Credentials (<i>username</i> only) are included in outbound SOAP request messages through a WS-Security UsernameToken header. No password is included. Message protection is provided using WS-Security 1.0'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>

Table 24–2 (Cont.) WSRP Producer Security Connection Parameters

Field	Description
Token Profile (cont.)	<ul style="list-style-type: none"> <li data-bbox="613 260 1365 642"> <p>■ WSS 1.0 Username Token With Password (oracle/wss10_username_token_with_message_protection_client_policy)—This policy provides username (with password) token profile based identity propagation with certificate based message protection for outbound SOAP requests in accordance with the WS-Security v1.0 standard. Both plain text and digest mechanisms are supported. This policy 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.</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.</p> <li data-bbox="613 659 1365 886"> <p>■ WSS 1.0 SAML Token (oracle/wss10_saml_token_client_policy)—This policy provides SAML-based authentication for outbound SOAP request messages in accordance with the WS-Security 1.0 standard. The policy propagates user identity and is typically used in intra departmental deployments where message protection and integrity checks are not required.</p> <p>This policy does not require any keystore configuration.</p> <li data-bbox="613 903 1365 1163"> <p>■ WSS 1.1 SAML Token with Message Protection (oracle/wss11_saml_token_with_message_protection_client_policy)—This policy provides message-level protection (integrity and confidentiality) and SAML token population for outbound SOAP requests in accordance with the WS-Security 1.1 standard. A SAML token, included in the SOAP message, is used in SAML-based authentication with sender vouches confirmation. This policy uses the symmetric key technology for signing and encryption, and WS-Security’s Basic 128 suite of asymmetric key technologies for endorsing signatures.</p> <li data-bbox="613 1180 1365 1226"> <p>■ None—No token. If None is selected, no WS-Security header is attached to the SOAP message.</p>
Configuration	<p>Select:</p> <ul style="list-style-type: none"> <li data-bbox="613 1285 1208 1310">■ Default to use a default token profile configuration. <li data-bbox="613 1327 1273 1377">■ Custom to provide a custom Oracle Web Service Manager configuration. <p>Additional security options display (including all the keystore properties) when you select Custom.</p>
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: WSS 1.0 SAML Token With Message Integrity, WSS 1.0 SAML Token With Message Protection. WSS 1.0 SAML Token, WSS 1.1 SAML Token with Message Protection</p>

Table 24–2 (Cont.) WSRP Producer Security Connection Parameters

Field	Description
Default User	<p>Enter a user name to assert to the remote producer when the user is not authenticated with the WebCenter Portal 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 it may be necessary to specify an alternative identity here. Keep in mind though, that in this case, the WebCenter Portal 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 remote WSRP producer must be set up to accept this information. You must also add a grant to the policy store as described in Section 24.2.3, "Adding a Grant to the Policy Store for a Mapped User Identity."</p> <p>Valid for: WSS 1.0 SAML Token With Message Integrity, WSS 1.0 SAML Token With Message Protection, WSS 1.0 SAML Token, WSS 1.1 SAML Token with Message Protection and WSS 1.0 Username Without Password.</p>
Associated External Application (Username With Password)	<p>If this producer uses an external application for authentication, use the Associated External Application dropdown list to identify the application. If the application you want is not listed, select Create New to define the external application now.</p> <p>An external application is required to support producers using the security option <i>WSS 1.0 Username With Password</i>. The external application stores and supplies the user credentials. See also Section 26.2, "Registering External Applications."</p> <p>Valid for: WSS 1.0 Username With Password only.</p>

- 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.

Only configure these properties if you want to override the configuration specified for the domain

For detailed parameter information, see [Table 24–3](#).

Table 24–3 WSRP Producer Key Store Connection Parameters

Field	Description
Recipient Alias	<p>Specify the key store alias that is associated with the producer's certificate.</p> <p>This certificate is used to encrypt the message to the producer.</p>
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 file specified must be created using JDK's keytool utility.</p>
Password	<p>Provide the password to the keystore that was set when the keystore was created. The producer is not available if a password is not specified or incorrect.</p>

Table 24–3 (Cont.) WSRP Producer Key Store Connection Parameters

Field	Description
Signature Key Alias	Enter the signature key alias. The Signature Key Alias 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 Signature Key Alias .
Encryption Key Alias	Enter the key alias used by the producer to encrypt the return message. A valid value is one of the key aliases that is located in the specified key store. This property is optional. If not specified, the producer uses the signing key for encrypting the return message.
Encryption Key Password	Enter the password for accessing the encryption key.

6. Click **OK**.

The new producer appears in the connection table.

24.2.2 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 Portal application. For command syntax and examples, see the section "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 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

24.2.3 Adding a Grant to the Policy Store for a Mapped User Identity

If you are using the `Default User` field to map an alternative user identity you must also add a grant to the policy store by doing one of the following:

- Adding the following grant directly to the policy store:

```
<grant>
  <grantee>
    <codesource>

    <url>file:${common.components.home}/modules/oracle.wsm.agent.common_11.1.1/wsm-
    agent.jar</url>
    </codesource>
  </grantee>
  <permissions>
    <permission>
      <class>oracle.wsm.security.WSIdentityPermission</class>
      <name>resource=MyAppID</name>
      <actions>assert</actions>
    </permission>
  </permissions>
</grant>
```


Replacing **MyAppID** in the line above with the name of the client application, including the version number if any.

- Granting the permission by running the following WLST command:

```
grantPermission(codeBaseURL='file:${common.components.home}/modules/oracle.wsm.agent.common_11.1.1/wsm-agent.jar',
permClass='oracle.wsm.security.WSIdentityPermission',
permTarget='resource=MyAppID', permActions='assert')
```

Replacing **MyAppID** with the name of the client application, including the version number if any.

24.2.4 Registering a WSRP Portlet Producer in WebCenter Portal: Spaces

For information about registering a WSRP portlet producer in WebCenter Portal: Spaces, see the section "Registering Portlet Producers Through Spaces Administration" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

24.2.5 Registering a WSRP Portlet Producer in WebCenter Portal: Framework Applications

For information about registering a WSRP portlet producer in Framework applications, see the section "How to Register a WSRP Portlet Producer" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

24.3 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 in 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
```

24.4 Registering Oracle PDK-Java Producers

This section describes how to register PDK-Java producers for a deployed WebCenter Portal application using Fusion Middleware Control and WLST commands. This section includes the following subsections:

- [Section 24.4.1, "Registering an Oracle PDK-Java Producer Using Fusion Middleware Control"](#)
- [Section 24.4.2, "Registering an Oracle PDK-Java Producer Using WLST"](#)

- [Section 24.4.3, "Registering an Oracle PDK-Java Portlet Producer in WebCenter Portal: Spaces"](#)
- [Section 24.4.4, "Registering an Oracle PDK-Java Portlet Producer in WebCenter Portal: Framework Applications"](#)

For information about how to register PDK-Java producers at design-time, using JDeveloper, see the section "How to Register an Oracle PDK-Java Portlet Producer" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

24.4.1 Registering an Oracle PDK-Java Producer Using Fusion Middleware Control

To register an Oracle PDK-Java portlet producer:

1. Log in to Fusion Middleware Control and navigate to the home page for the WebCenter Portal application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
3. In the **Add Portlet Producer Connection** section, enter connection details for the Oracle PDK-Java producer.

For detailed parameter information, see [Table 24-4, "Oracle PDK-Java Producer Connection Parameters"](#).

Table 24-4 Oracle PDK-Java Producer Connection Parameters

Field	Description
Connection Name	Enter a unique name that identifies this portlet producer registration within the WebCenter Portal application. The name must be unique across all WebCenter Portal connection types. The name you specify here appears in Composer (under the <i>Portlets</i> folder).
Producer Type	Indicate the type of this producer. Select Oracle PDK-Java Producer .
URL End Point	Enter the Oracle PDK-Java producer's URL using the following syntax: <code>http://host_name:port_number/context_root/providers</code> Where: <ul style="list-style-type: none"> ■ <code>host_name</code> is the server where the producer is deployed ■ <code>port_number</code> is the HTTP Listener port number ■ <code>context_root</code> is the Web application's context root ■ <code>providers</code> is static text For example: <code>http://myHost.com:7778/myEnterprisePortlets/providers</code>

Table 24–4 (Cont.) Oracle PDK-Java Producer Connection Parameters

Field	Description
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.example.com:7778/xyz/providers</pre> <p>However, the following URL endpoint, does not require a service ID:</p> <pre>http://domain.example.com:7778/xyz/providers/sample</pre> <p>The service ID is used to look up a file called <code><service_id>.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.properties</code> is used.</p>
Use Proxy?	<p>Select this checkbox if the WebCenter Portal application must use an HTTP proxy when contacting this producer. If selected, enter values for Proxy Host and Proxy Port.</p> <p>A proxy is required if the WebCenter Portal 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 or IP address of 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. The default port is 80.</p>
Associated External Application	<p>If one of this producer's portlets requires authentication, use the Associated External Application dropdown to identify the correct external application.</p> <p>If the application you want is not listed, select Create New to define the external application now.</p> <p>See also Section 26.2, "Registering External Applications."</p>
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 you specify a shared key, you must also select this option.</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 communications with the producer, in seconds. For example, the maximum time the producer may take to register, deregister, or display portlets on WebCenter Portal application 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>

Table 24–4 (Cont.) Oracle PDK-Java Producer Connection Parameters

Field	Description
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 Portal 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 fails 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 the Federated Portal Adapter (FPA). The Shared Key is also known as the HMAC key.</p>

4. Click **OK**.

The new producer appears in the connection table.

24.4.2 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 Portal application. For command syntax and examples, see the section "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 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

24.4.3 Registering an Oracle PDK-Java Portlet Producer in WebCenter Portal: Spaces

For information about registering an Oracle PDK-Java portlet producer in WebCenter Portal: Spaces, see the section "Registering Portlet Producers Through Spaces Administration" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

24.4.4 Registering an Oracle PDK-Java Portlet Producer in WebCenter Portal: Framework Applications

For information about registering an Oracle PDK-Java portlet producer in Framework applications, see the section "How to Register an Oracle PDK-Java Portlet Producer" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

24.5 Testing Oracle PDK-Java Producer Connections

To verify an Oracle PDK-Java producer connection, run the producer URL in a browser window in the following format:

```
http://host_name:port_number/context-root/providers/producer_name
```

For example:

```
http://domain.example.com:7778/xyz/providers/sample
```

24.6 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 an Oracle PDK-Java producer

To retain all the portlet customizations and personalizations that users make while working with WebCenter Portal applications, you must also migrate producer customizations and personalizations to the producer's new location. Use the WLST commands `exportPortletClientMetadata` and `importPortletClientMetadata` to migrate portlet client metadata to a different location. For more information, see [Section 39.2.3, "Exporting Portlet Client Metadata \(Framework Applications\)"](#) and [Section 39.2.4, "Importing Portlet Client Metadata \(Framework Applications\)"](#).

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. For more information, see [Section 39.1.3.13, "Exporting Portlet Producers"](#) and [Section 39.1.3.14, "Importing Portlet Producers."](#)

This section includes the following subsections:

- [Section 24.6.1, "Editing Producer Registration Details Using Fusion Middleware Control"](#)
- [Section 24.6.2, "Editing Producer Registration Details Using WLST"](#)
- [Section 24.6.3, "Migrating WSRP Producer Metadata to a New WSDL URL"](#)

24.6.1 Editing Producer Registration Details Using Fusion Middleware Control

To update connection details for a portlet producer:

1. Log in to Fusion Middleware Control and navigate to the home page for the WebCenter Portal application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:

- For the Spaces application - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
- For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
3. From the list of services on the WebCenter Portal Service Configuration page, select **Portlet Producers**.
4. In the **Manage Portlet Producer Connections** section, select the producer you want to modify, and click **Edit**.
5. In the **Edit Portlet Producer Connection** section, modify connection details, as required. For more information, see:
 - [Table 24–1, "WSRP Producer Connection Parameters"](#)
 - [Table 24–4, "Oracle PDK-Java Producer Connection Parameters"](#)
6. Click **OK**.

24.6.2 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 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

24.6.3 Migrating WSRP Producer Metadata to a New WSDL URL

If you want to move a WSRP producer to a new WSDL URL, you can use the `exportPortletClientMetadata`, `setWSRPProducer`, and `importPortletClientMetadata` WLST commands to migrate the existing producer metadata to the new location.

To migrate WSRP producer metadata to a new URL endpoint:

1. Export the producer metadata, using the WLST command `exportPortletClientMetadata`. For command syntax and examples, see "exportPortletClientMetadata" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.
2. Change the producer's WSDL URL, using the WLST command `setWSRPProducer`. For command syntax and examples, see "setWSRPProducer" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.
3. Import the producer metadata, using the WLST command `importPortletClientMetadata`. For command syntax and examples, see "importPortletClientMetadata" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

24.7 Deregistering Producers

You can deregister producers at any time but, before doing so, consider any impact to the WebCenter Portal application as portlets associated with a deregistered producer

no longer work. Check the *Portlets Producer Invocation* metric to see how frequently the producer is being used. For more information, see [Section 38.2, "Viewing Performance Information."](#)

When you deregister a producer, registration data is removed from both the WebCenter Portal application and the remote producer:

- WebCenter Portal application - The 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 Portal application pages. In place of the portlet, users 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 26.5, "Deleting External Application Connections."](#)

This section includes the following subsections:

- [Section 24.7.1, "Deregistering Producers Using Fusion Middleware Control"](#)
- [Section 24.7.2, "Deregister Producers Using WLST"](#)
- [Section 24.7.3, "Deregistering Producers in WebCenter Portal: Spaces"](#)
- [Section 24.7.4, "Deregistering Producers in WebCenter Portal: Framework Applications"](#)

24.7.1 Deregistering Producers Using Fusion Middleware Control

To deregister a portlet producer:

1. Log in to Fusion Middleware Control and navigate to the home page for the WebCenter Portal application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. Do one of the following:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
3. From the list of services on the WebCenter Portal Service Configuration page, select **Portlet Producers**.
4. Select the name of the producer you want to remove, and click **Delete**.

The connection details are removed. Portlets associated with this producer are no longer accessible within the WebCenter Portal application.

24.7.2 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 the out-of-the-box or sample producers provided with Oracle WebCenter Portal:

- **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 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

24.7.3 Deregistering Producers in WebCenter Portal: Spaces

For information about deregistering portlet producers in WebCenter Portal: Spaces, see the section "Deregistering Portlet Producers" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

24.7.4 Deregistering Producers in WebCenter Portal: Framework Applications

For information about deregistering portlet producers in Framework applications, see the section "How to Delete a Portlet Producer" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

24.8 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, or WLST. For information on deploying a portlet producer at design-time, through Oracle JDeveloper, see the chapter "Testing and Deploying Your Portlets" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

This section includes the following subsections:

- [Section 24.8.1, "Understanding Portlet Producer Application Deployment"](#)
- [Section 24.8.2, "Converting a JSR 286 Portlet Producer EAR File into a WSRP EAR File"](#)
- [Section 24.8.3, "Deploying Portlet Producer Applications Using Oracle JDeveloper"](#)
- [Section 24.8.4, "Deploying Portlet Producer Applications Using Fusion Middleware Control"](#)
- [Section 24.8.5, "Deploying Portlet Producer Applications Using Oracle WebLogic Server Administration Console"](#)
- [Section 24.8.6, "Deploying Portlet Producer Applications Using WLST"](#)

For more information about deploying applications, see the chapter "Deploying Application" in *Oracle Fusion Middleware Administrator's Guide*.

24.8.1 Understanding Portlet Producer Application Deployment

You can deploy your Portlet Producer application to any Oracle WebLogic Managed Server instance that is configured to support WebCenter Portal portlet producers. To deploy an application to a managed server, you can use Oracle Enterprise Manager Fusion Middleware Control, Oracle WebLogic Administration Console, or WLST. For

more information about these administration tools, see [Section 1.13, "Oracle WebCenter Portal Administration Tools."](#)

24.8.2 Converting a JSR 286 Portlet Producer EAR File into a WSRP EAR File

To deploy JSR 286 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 286 portlet producer EAR file into a WSRP EAR file, run the WSRP producer predeployment tool located in the Middleware directory at

`WC_ORACLE_HOME/webcenter/modules/oracle.portlet.server_11.1.1`, as follows:

```
java -jar wsrp-predeploy.jar source EAR target EAR
```

For JSR 286 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 `WC_ORACLE_HOME/webcenter/modules/oracle.portlet.server_11.1.1` directory.
- `source EAR` is the name of the JSR 286 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 286 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.

24.8.3 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, if 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 the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

24.8.4 Deploying Portlet Producer Applications Using Fusion Middleware Control

For information about deploying a portlet producer application using Fusion Middleware Control, see [Section 7.1.6.4, "Deploying Applications Using Fusion Middleware Control."](#)

24.8.5 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 7.1.6.6, "Deploying Applications Using the WLS Administration Console."](#)

24.8.6 Deploying Portlet Producer Applications Using WLST

For information on deploying a portlet application using the WLST command, see [Section 7.1.6.5, "Deploying Applications Using WLST."](#)

24.9 Configuring WebCenter Services Portlets

WebCenter Portal provides social networking and personal productivity features through services, which, in turn, expose subsets of their features and functionality through task flows. These services and task flows are readily available for use in the Spaces application and other WebCenter Portal applications. However, application developers using other products, such as Oracle Portal, Oracle WebLogic Portal, and Oracle WebCenter Interaction, may also want to expose these same features within those applications.

WebCenter Services Portlets is a preconfigured, out-of-the-box producer that enables you to expose WebCenter Portal service task flows to other applications as WSRP portlets or pagelets.

The following task flows are provided as portlets by WebCenter Services Portlets:

- Document Manager—Displays folders, files, and wikis from the WebCenter Content repository
- Blogs—Displays blog posts from a selected location in the WebCenter Content repository
- Discussion Forums—Displays all discussions and their respective replies and enables users to perform various operations based on their privileges
- Announcements—Displays all current announcements and enables users to perform various operations based on their privileges
- Lists—Displays user-created lists and provides controls for creating lists and adding list data

- Polls Manager—Enables users to perform administrative operations on polls
- Take Polls—Displays the most recently published available poll, or a specific poll identified by the pollId parameter
- Worklist—Enables users to view and take action on all tasks and notifications from one or more Oracle BPEL Server
- Mail—Displays a mail inbox
- Activity Stream—Provides an overview of the most recent activities performed by a user's connections
- Tag Cloud—Displays a tag cloud, which is a visual depiction of all the tags used on the page

WebCenter Services Portlets starts life as a Framework application. This application includes several pages, one for each of the exposed task flows. The application is then portletized, using the Oracle JSF Portlet Bridge, and deployed to the WC_Portlet managed server.

After installation of WebCenter Portal, WebCenter Services Portlets is automatically available for use. However, for the portlets and pagelets to work correctly there are some configuration steps that must be completed.

This section includes the following subsections:

- [Section 24.9.1, "Configuring Service Back-End Connections"](#)
- [Section 24.9.2, "Configuring Security for WebCenter Services Portlets"](#)
- [Section 24.9.3, "Troubleshooting WebCenter Services Portlets"](#)

24.9.1 Configuring Service Back-End Connections

Most of the services included in WebCenter Services Portlets require connections to back-end servers to be fully functional. For example, the Documents service requires a connection to an Oracle WebCenter Content repository and the Discussions and Announcements services require a connection to a discussions server for Oracle WebCenter Portal. These connections must be configured before application developers can start to consume the portlets and pagelets provided by the producer.

This section includes the following subsections:

- [Section 24.9.1.1, "Configuring the Documents Service Content Repository Connection"](#)
- [Section 24.9.1.2, "Configuring the Worklist Service Connection"](#)
- [Section 24.9.1.3, "Configuring the Discussions and Announcements Services Connection"](#)
- [Section 24.9.1.4, "Configuring the Mail Service Connection"](#)

24.9.1.1 Configuring the Documents Service Content Repository Connection

WebCenter Services Portlets includes portlets for task flows provided by the Documents, Blog, and Wiki services. These portlets require a connection to a back-end WebCenter Content repository.

For general information about configuring WebCenter Content, see [Chapter 11, "Managing Content Repositories."](#)

There are two ways to create a connection to a WebCenter Content repository:

- Using Fusion Middleware Control. For more information, see [Section 11.6.2, "Registering Content Repositories Using Fusion Middleware Control."](#)
- Using the WLST command line tool. For more information, see [Section 11.6.3, "Registering Content Repositories Using WLST."](#)

Note: WebCenter Services Portlets uses the WebCenter Content repository identified as the active or default connection, so you must ensure that you have set the appropriate connection as the default. For more information, see [Section 11.7, "Changing the Active \(or Default\) Content Repository Connection."](#)

24.9.1.2 Configuring the Worklist Service Connection

WebCenter Services Portlets includes portlets for the Worklist task flow provided by the Worklist service. The Worklist service requires connections to every Oracle BPEL Server from which you want to monitor worklist items.

For general information about configuring the Oracle BPEL Server and the Worklist service, see [Chapter 23, "Managing the Worklist Service."](#)

There are two ways to create a connection to an Oracle BPEL Server:

- Using Fusion Middleware Control. For more information, see [Section 23.4.2.1, "Registering Worklist Connections Using Fusion Middleware Control"](#)
- Using the WLST command line tool. For more information, see [Section 23.4.2.2, "Registering Worklist Connections Using WLST."](#)

24.9.1.3 Configuring the Discussions and Announcements Services Connection

WebCenter Services Portlets includes portlets for task flows provided by the Discussions and Announcements services. These services require a connection to a back-end discussions server for Oracle WebCenter Portal. Both services use the same connection. Oracle WebCenter Portal's discussion server is installed automatically with Oracle Fusion Middleware, but you must create the connection to the server.

For general information about configuring the Discussions and Announcements services, see [Chapter 14, "Managing the Announcements and Discussions Services."](#)

There are two ways to create a connection to an Oracle WebCenter Portal Discussions server:

- Using Fusion Middleware Control. For more information, see [Section 14.3.1, "Registering Discussions Servers Using Fusion Middleware Control."](#)
- Using the WLST command line tool. For more information, see [Section 14.3.2, "Registering Discussions Servers Using WLST."](#)

Note: WebCenter Services Portlets uses the discussions server identified as the active or default connection, so you must ensure that you have set the appropriate connection as the default. For more information, see [Section 14.4, "Choosing the Active Connection for Discussions and Announcements."](#)

24.9.1.4 Configuring the Mail Service Connection

WebCenter Services Portlets includes portlets for the Mail task flow provided by the Mail service. This service requires a connection to a back-end mail server. This server

can be the Microsoft Exchange Server or any mail server that supports IMAP4 and SMTP.

For general information about configuring the Mail service, see [Chapter 17, "Managing the Mail Service."](#)

There are two ways to create a connection to your mail server:

- Using Fusion Middleware Control. For more information, see [Section 17.4.1, "Registering Mail Servers Using Fusion Middleware Control."](#)
- Using the WLST command line tool. For more information, see [Section 17.4.2, "Registering Mail Servers Using WLST."](#)

Note: WebCenter Services Portlets uses the mail server identified as the active or default connection, so you must ensure that you have set the appropriate connection as the default. For more information, see [Section 17.5, "Choosing the Active \(or Default\) Mail Server Connection."](#)

24.9.2 Configuring Security for WebCenter Services Portlets

WebCenter Services Portlets should be secured to ensure that users cannot access information that they do not have privileges to access. As a WSRP producer, WebCenter Services Portlets uses WS-Security to ensure identity propagation.

For information about how to configure WS-Security for a WSRP portlet producer, see [Section 35.1, "Securing a WSRP Producer."](#)

Note: After attaching the required security policy, you must restart the WC_Portlet managed server.

24.9.3 Troubleshooting WebCenter Services Portlets

This section includes the following subsections:

- [Section 24.9.3.1, "Rich Text Editor Not Working for Document Manager and Blogs Portlets"](#)
- [Section 24.9.3.2, "Cannot Manage Lists in the Lists Portlet"](#)
- [Section 24.9.3.3, "Portlet Uses Incorrect Time Zone or Date and Time Format"](#)
- [Section 24.9.3.4, "Portlet Displays Remote Portlet Communication Error"](#)

24.9.3.1 Rich Text Editor Not Working for Document Manager and Blogs Portlets

Blogs and wikis use a rich text editor (CKEditor) that requires access to various resources at runtime.

If the WebCenter Services Portlets producer is behind a firewall that the end-user browser cannot get through, the URLs for the resources required by CKEditor cannot be accessed and the editor will not display in the Blogs portlet or in the Document Manager portlet when viewing wikis.

To resolve this issue:

1. Create an application that includes the CKEditor resources, for example by using WebCenter Portal's Framework application template.

2. Deploy the application to the same server that is used by the application that is consuming WebCenter Services Portlets.
3. Run the WebCenter Services Portlets producer application.
4. In the WebCenter Portal Administration Console, edit the **Base Resource URL** to point to the new application.
For more information about how to do this, see [Section 36.3.5, "Choosing the Default Base Resource URL."](#)
5. Refresh the browser displaying the consumer application. The rich text editor should now display correctly as the CKEditor resources are available on the same side of the firewall as the consumer application.

24.9.3.2 Cannot Manage Lists in the Lists Portlet

Out of the box, only users who are members of the `Administrator` role can create, edit, and delete lists and edit list data. If a user is not a member of the `Administrator` role, he or she will only be able to view lists.

To enable a user who is not a member of the `Administrator` role to manage lists, use Fusion Middleware Control to assign the user the `manage` permission on the `ListPermission` role:

```
<permission>
  <class>oracle.webcenter.list.model.security.ListPermission</class>
  <name>/oracle/webcenter/list/templates/lists/.*</name>
  <actions>manage</actions>
</permission>
```

1. In Fusion Middleware Control, under **Application Deployments**, right-click the **services-producer** application and choose **Security** and then **Application Policies** from the context menu.
2. Click **Create**.
3. In the Grantee section, click **Add**.
4. In the Add Principal dialog, locate the user or role to which you want to add the list permission.
5. Click **OK**.
6. In the Permissions section, click **Add**.
7. In the Add Permission dialog, from the **Permission Class** dropdown list, select **oracle.webcenter.list.model.security.ListPermission**.
8. Click the **Search system security grants** icon.
9. In the Search Results section, select the **Resource Name** with the **manage Permission Action**.
10. Click **Continue**.
11. In the confirmation dialog, click **Select** to confirm the permission for the target user or role.
12. Click **OK**.

24.9.3.3 Portlet Uses Incorrect Time Zone or Date and Time Format

Currently, user preferences are not propagated from the portlet consumer to the WebCenter Services Portlets producer. This means that WebCenter Services Portlets

always use the time zone and date and time format preferences set on the server where the producer is deployed, regardless of the settings users specify in the consumer application.

24.9.3.4 Portlet Displays Remote Portlet Communication Error

If a portlet provided by WebCenter Services Portlets displays a Remote Portlet Communication Error, this is typically because the WS-Security was not configured on the producer.

For information about how to resolve this problem, see [Section 24.9.2, "Configuring Security for WebCenter Services Portlets."](#)

24.10 Troubleshooting Portlet Producer Issues

This section includes the following sub sections:

- [Section 24.10.1, "Producer Registration Fails for a WebCenter Portal: Framework Application"](#)
- [Section 24.10.2, "Portlet Unavailable: WSM-00101 Exception"](#)

24.10.1 Producer Registration Fails for a WebCenter Portal: Framework 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 24.3, "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 Framework application" in the chapter "Consuming Portlets" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*, and redeploy the application, as described in [Section 7.1, "Deploying Framework 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>

```

24.10.2 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 Portal 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 35.1.3, "Setting Up the Keystores."](#)

Managing Oracle WebCenter Portal's Pagelet Producer

Oracle WebCenter Portal's Pagelet Producer (previously called Oracle WebCenter Ensemble) provides a collection of useful tools that facilitate dynamic pagelet development and deployment. The Pagelet Producer proxy provides users with external access to internal resources including internal applications and secured content. Using the Pagelet Producer, you can expose WSRP and Oracle JPDK portlets and OpenSocial gadgets as pagelets for use in any web page or application.

This chapter describes how to register, edit and deploy pagelets using the Pagelet Producer Administrative Console.

This chapter includes the following sections:

- [Section 25.1, "About the Pagelet Producer"](#)
- [Section 25.2, "Registering the Pagelet Producer"](#)
- [Section 25.3, "Configuring Pagelet Producer Settings"](#)
- [Section 25.4, "Creating Resources"](#)
- [Section 25.5, "Creating Pagelets"](#)
- [Section 25.6, "Creating Web Injectors"](#)
- [Section 25.7, "Creating Custom Parsers"](#)
- [Section 25.8, "Creating Hosted Files"](#)
- [Section 25.9, "Registering WSRP and Oracle JPDK Portlet Producers"](#)
- [Section 25.10, "Troubleshooting"](#)

Audience

The content of this chapter is intended for Fusion Middleware administrators. For more information, see [Section 1.13, "Oracle WebCenter Portal Administration Tools."](#)

25.1 About the Pagelet Producer

This section is an introduction to Pagelet Producer concepts and features and includes the following topics:

- [Section 25.1.1, "Key Concepts"](#)
- [Section 25.1.2, "Support for WSRP and Oracle JPDK Portlets"](#)
- [Section 25.1.3, "Support for OpenSocial Gadgets"](#)

- [Section 25.1.4, "Support for Oracle WebCenter Interaction Portlets"](#)

25.1.1 Key Concepts

The following key concepts are useful when working with the Pagelet Producer:

- The **Pagelet Producer Console** is a browser-based administration tool used to create and manage the various objects in your Pagelet Producer deployment. From the Console you can register web applications as resources and create pagelets, manage proxy and transformation settings, and more.

The Pagelet Producer Console is accessible through any web browser at the following URL: **`http://<host_name>:<port_number>/pagelets/admin`**.

Any user with the 'Admin' role on the host application server can access the Pagelet Producer Console. To grant administrative access to the Pagelet Producer Console to users without administrative access to the application server, use the 'EnsembleAdmin' role.

The Pagelet Producer Console can also be launched in accessible mode at: `http://<host_name>:<port_number>/pagelets/accessible`.

- **Resources** are core objects used to register applications within the Pagelet Producer, including stand-alone web applications, Portlet Producers and OpenSocial containers. Creating a resource allows the proxy to map internal applications to external URLs, manage authentication, and transform applications. Registering a web application as a Pagelet Producer resource allows you to do the following:

- Proxy internal web applications to external addresses.
- Manage authentication, both at the proxy level and at the resource level.
- Transform proxied web applications, including URL rewriting.

- **Pagelets** are sub-components of a web page accessed through the Pagelet Producer that can be injected into any proxied application. Any application on a Pagelet Producer resource that returns markup can be registered as a pagelet, which can then be displayed in Oracle WebCenter Portal, Spaces, or any web application.

A pagelet is a reusable user interface component similar to a portlet. While portlets were designed specifically for portals, pagelets are designed to run on any web page. Any HTML fragment can be a pagelet. Pagelet developers can create pagelets that are parameterized and configurable, dynamically interact with other pagelets, and respond to user input using Asynchronous Javascript and XML (AJAX) patterns.

Pagelet Producer registration is dynamic. Additions and updates to existing producers are immediately available; in most cases, it is not necessary to restart the WebCenter Portal application or the managed server.

Note: In the current release, only a single administrator can modify Pagelet Producer administrative settings at any given time. Concurrent edits will result in only one edit succeeding. However, data integrity will always be preserved.

25.1.2 Support for WSRP and Oracle JPDK Portlets

Using the Pagelet Producer, you can expose WSRP and Oracle JPDK portlets as pagelets for use in any web page or application.

After setting up the Pagelet Producer as described in [Section 25.2, "Registering the Pagelet Producer,"](#) follow the steps below to import WSRP or Oracle JPDK portlets:

1. Register the portlet producer with the Pagelet Producer as described in [Section 25.9, "Registering WSRP and Oracle JPDK Portlet Producers."](#)
2. This automatically creates a resource and pagelets in the Pagelet Producer Console based on the portlet definitions for the producer. For details on the resource settings, see [Section 25.4, "Creating Resources."](#)
3. To modify the imported resource or the associated pagelets, you must make a copy of the imported resource; for details, see [Section 25.9.3, "Using WSRP and Oracle JPDK Portlets."](#)

25.1.3 Support for OpenSocial Gadgets

Using the Pagelet Producer, you can expose OpenSocial gadgets as pagelets for use in any web page or application.

After setting up the Pagelet Producer as described in [Section 25.2, "Registering the Pagelet Producer,"](#) follow the steps below to import OpenSocial gadgets:

1. Define the OpenSocial container as described in [Section 25.3.6, "OpenSocial Settings."](#)
2. Create an OpenSocial resource in the Pagelet Producer Console as described in [Section 25.4, "Creating Resources"](#) and [Section 25.4.3, "Configuration Pages for OpenSocial Resources \(OpenSocial Gadget Producers\)."](#)
3. Create pagelets for OpenSocial gadgets as described in [Section 25.5, "Creating Pagelets."](#) The Pagelet Producer Console allows you to import gadget metadata from OpenSocial to populate the pagelet settings.

25.1.4 Support for Oracle WebCenter Interaction Portlets

The Pagelet Producer can be used as a portlet provider for Oracle WebCenter Interaction. There are several configuration pages that allow you to define CSP settings for use with Oracle WebCenter Interaction:

1. Configure the Pagelet Producer settings for use with the Oracle WebCenter Interaction Credential Mapper, SOAP API service and image service, see the [CSP Settings](#) in [Section 25.3, "Configuring Pagelet Producer Settings."](#)
2. Set up the Pagelet Producer's connection to the server hosting the portlet code by creating a CSP resource as described in [Section 25.4, "Creating Resources."](#)
3. Create pagelets for the Oracle WebCenter Interaction portlets as described in [Section 25.5, "Creating Pagelets."](#)

25.2 Registering the Pagelet Producer

This section describes how to register and configure the Pagelet Producer using Fusion Middleware Control and WLST commands. This section includes the following subsections:

- [Section 25.2.1, "Registering the Pagelet Producer for WebCenter Portal Applications Using Fusion Middleware Control"](#)
- [Section 25.2.2, "Registering the Pagelet Producer for WebCenter Portal Applications Using WLST"](#)
- [Section 25.2.3, "Configuring the Pagelet Producer Service"](#)
- [Section 25.2.4, "Registering Pagelet Producer Using WebCenter Portal: Spaces"](#)

25.2.1 Registering the Pagelet Producer for WebCenter Portal Applications Using Fusion Middleware Control

To register the Pagelet Producer:

1. Log in to Fusion Middleware Control and navigate to the home page for your WebCenter Portal application. For more information, see:
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#).
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
2. Do one of the following:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **Register Producer**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal**, then **Register Producer**.
3. Enter connection details for the Pagelet Producer ([Table 25–1](#)).

Table 25–1 Pagelet Producer Connection Parameters

Field	Description
Connection Name	Enter a unique name to identify this Pagelet Producer instance within the WebCenter Portal application. The name must be unique across all WebCenter Portal connection types. The name specified here appears in Composer under the Mash-ups > Pagelet Producers folder (by default).
Producer Type	Select Pagelet Producer .
Server URL	<p>Enter the URL of the Pagelet Producer. The URL must include a fully-qualified domain name. Use the following syntax:</p> <pre><protocol>://<host_name>:<port_number>/pagelets/</pre> <p>For example:</p> <pre>http://myhost.com:7778/pagelets/</pre> <p>If pagelets contain secure data, the registered URL must use the https protocol. For example:</p> <pre>https://myhost.com:7779/pagelets/</pre> <p>The context root can be changed from /pagelets/ if necessary; for details, see Section 25.3, "Configuring Pagelet Producer Settings."</p> <p>Note: In Spaces, if the Pagelet Producer URL is protected by OAM, the URL to the pagelet catalog must be excluded (mapped directly without access control), or the catalog will appear to be empty when using REST. The pagelet catalog URL is <code>http://<host_name>:<port_number>/pagelets/api/v2/ensemble/pagelets</code></p>

4. Click **OK**. The new producer appears in the connection table.

25.2.2 Registering the Pagelet Producer for WebCenter Portal Applications Using WLST

Use the `registerPageletProducer` command to register a Pagelet Producer for your WebCenter Portal application. For command syntax and examples, see the section "registerPageletProducer" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

You can also use WLST to list or edit the current connection details.

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

25.2.3 Configuring the Pagelet Producer Service

This section describes how to set up the Pagelet Producer for use as a service by Oracle WebCenter Portal using the Oracle Configuration Wizard.

For information about developing and deploying pagelets, see the section "Creating Pagelets with Oracle WebCenter Portal's Pagelet Producer" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

To set up the Pagelet Producer as a WebCenter Portal service:

1. Launch the **Configuration Wizard (Oracle Fusion Middleware > Oracle WebLogic Server > Tools > Configuration Wizard)**.
2. Select **Create a new WebLogic Domain**. Click **Next**.
3. Select **Base this domain on an existing template** and select the **Pagelet Producer domain template**. Confirm that the template location is correct and click **Next**.
4. Complete the domain configuration wizard. For details, see the online help.

All post deployment connection configuration is stored in the Oracle Metadata Services (MDS) repository. For more information, see [Section 1.3.5, "WebCenter Portal Configuration Considerations."](#) For detailed information about MDS, see the chapter "Managing the Oracle Metadata Repository" in the *Oracle Fusion Middleware Administrator's Guide*.

The Pagelet Producer stores all configuration data on a separate partition in the MDS schema of RCU. Typically, this schema is installed as part of the Oracle WebCenter Portal installation. This configuration data does not conflict with data that belongs to other services. When the Pagelet Producer domain template is deployed, the wizard prompts for connectivity information to the database in which the schema has been created. The names that the Pagelet Producer expects are:

- Datasource Name: `mds-PageletProducerDS`
- JNDI name: `jdbc/mds/PageletProducerDS`
- MDS partition name: `pageletproducer`

To use OpenSocial gadgets in conjunction with WebCenter Portal profile and activities features, you must manually configure the `WebCenterDS` data source to target the `WC_Portlet` server.

1. In the Oracle WebLogic Server Console, go to **Services > Data Source**.
2. Click on the **WebCenterDS** data source.
3. Go to the **Targets** tab.
4. Select the **WC_Portlet** server and click **Save**.

25.2.4 Registering Pagelet Producer Using WebCenter Portal: Spaces

This section explains how to register the Pagelet Producer in WebCenter Portal: Spaces.

1. Log in to Spaces and click **Administration**.
2. Navigate to the **Configuration** tab and click **Services**.
3. On the Services and Providers page, click **Portlet Producers**.
4. Click **Register** and select **Pagelet Producer**.
5. Enter the following information:
 - **Producer Name:** Used to identify the Pagelet Producer registration in Spaces.
 - **Server URL:** URL to the Pagelet Producer in the format `http://host:port/pagelets` (where host and port correspond to the WC_Portlet managed server where the Pagelet Producer is configured).

25.3 Configuring Pagelet Producer Settings

The Settings section in the Pagelet Producer Console provides access to important configuration settings that affect all Pagelet Producer resources. For an introduction to the Pagelet Producer Console, see [Section 25.1, "About the Pagelet Producer."](#)

The following pages are included in the Settings section:

- [Section 25.3.1, "Logging Settings"](#)
- [Section 25.3.2, "Proxy Settings"](#)
- [Section 25.3.3, "Transform Settings"](#)
- [Section 25.3.4, "CSP Settings"](#)
- [Section 25.3.5, "Kerberos Settings"](#)
- [Section 25.3.6, "OpenSocial Settings"](#)

25.3.1 Logging Settings

The Logging page allows you to set logging levels for Pagelet Producer components.

Figure 25–1 Pagelet Producer Console: Settings - Logging



To enable logging for any component, choose one of the following logging levels:

- Severe
- Warning
- Info
- Config
- Fine
- Finer
- Finest

Logging messages can be viewed in the managed server log files. In Oracle WebLogic Server, this would be *domain_home/servers/managed_server_name/managed_server_name.log* and *managed_server_name-diagnostic.log*.

25.3.2 Proxy Settings

The Proxy page allows you to define a semicolon-separated list of URLs that will not be proxied (wildcards are allowed), and set the HTTP proxy configuration if necessary (URL, user name and password).

You must restart the Pagelet Producer after changing the proxy settings.

Note: If an HTTP proxy is required for external connections in the deployment environment, initial server startup will report connection errors. These errors are not an indication of problems with the environment; they indicate that some external OpenSocial libraries cannot be loaded remotely. The errors can be resolved by configuring the proxy settings as described above and restarting the server.

Note for Oracle WebLogic Server deployments: The HTTP Proxy Server URL entered on the Proxy page is applied to all applications running on the server that hosts the Pagelet Producer (on Oracle WebLogic Server, this setting is applied to all applications running on the WC_Portlet managed server). Oracle WebLogic Server users should pay particular attention to this setting and make sure that the WLS Administrative Server host and all clustered managed servers are included in the "Do not proxy hosts" list.

Figure 25–2 Pagelet Producer Console: Settings - Proxy

ORACLE WebCenter Portal: Pagelet Producer

Navigator

Jump to: Settings

- Logging
- Proxy**
- Transform
- CSP
- Kerberos
- OpenSocial

Do not proxy hosts

HTTP Proxy Server Password

HTTP Proxy Server URL

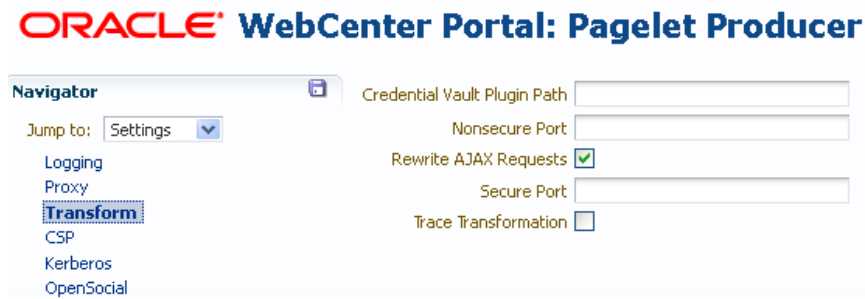
HTTP Proxy Server Username

25.3.3 Transform Settings

The Transform page allows you to enter the path to the credential vault provider and configure secure and insecure ports for the Pagelet Producer. This page also allows you to choose whether or not to intercept and transform Ajax requests, and whether or not to log pre- and post- transformation content (this option can be useful for debugging, but should not be enabled in a production environment).

Note: The Nonsecure Port defaults to 8889. If the Pagelet Producer is deployed on a different port, change this entry and restart the server.

Figure 25–3 Pagelet Producer Console: Settings - Transform



25.3.4 CSP Settings

CSP is a platform-independent protocol based on the open standard of HTTP 1.1. CSP defines the syntax of communication between the Pagelet Producer and external resources. It also defines custom headers as well as outlines how services use HTTP to communicate and modify settings.

This page allows you to configure the Oracle WebCenter Interaction Credential Mapper, SOAP API service, and image service.

Note: This page may be ignored if Oracle WebCenter Interaction is not present in your deployment. These settings are used for backwards compatibility with CSP portlets written for Oracle WebCenter Interaction.

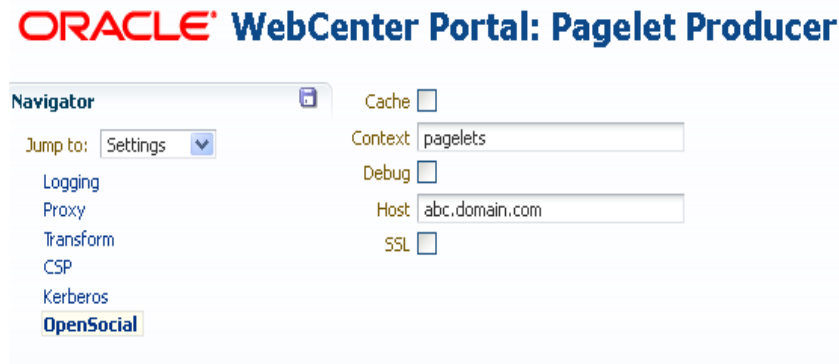
25.3.5 Kerberos Settings

This page is used to define the paths to the Kerberos configuration files (java.security.krb5.conf and java.security.auth.login.conf). These two configuration files are needed to configure the Kerberos realm and KDC to instruct HTTPClient where to retrieve the Kerberos Service ticket.

25.3.6 OpenSocial Settings

This page allows you to configure the Pagelet Producer for use with OpenSocial gadgets.

Figure 25–4 Pagelet Producer Console: Settings - OpenSocial



This page includes the following settings:

- The **Context** field defines the context to which the Pagelet Producer is deployed. This value should be left at the default setting ("pagelets") unless a change is required by the OpenSocial container.
- The **Host** field should contain the fully-qualified domain name of Pagelet Producer host. This value should be retrieved automatically from the environment; if it is not, restart the server to pick up the correct configuration settings. As with the Context setting, this value should be left at the default unless a change is required by the OpenSocial container.
- The **Cache** option enables Pagelet Producer internal caching for OpenSocial gadgets.
- The **Debug** option enables debugging for OpenSocial gadgets (disables JavaScript obfuscation).
- The **SSL** option enables SSL for OpenSocial gadgets.

Note: You must also configure the secure (HTTPS) and nonsecure (HTTP) ports before importing OpenSocial gadgets. For details on these settings, see [Section 25.3.3, "Transform Settings."](#)

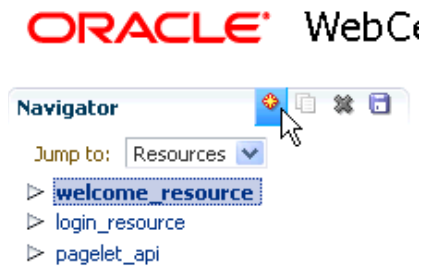
25.4 Creating Resources

As noted in [Section 25.1, "About the Pagelet Producer,"](#) resources are applications registered with the Pagelet Producer. Registering an application as a resource allows the proxy to map internal applications to external URLs, manage authentication, and transform application functionality.

To create a new resource, use the steps below:

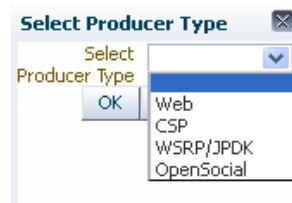
1. Select the **Resources** option from the dropdown list in the Pagelet Producer Console navigator.
2. Click on any existing resource and click the **Create** icon in the navigator toolbar. (This button is only enabled when you have selected an object type that can be created.)

Figure 25–5 Pagelet Producer Console - Create Resource



3. In the **Select Producer Type** dialog box, choose the type of producer that the resource will be configured to proxy from the dropdown list:
 - **Web**: Any standard web application
 - **CSP**: CSP portlet provider application (for use with Oracle WebCenter Interaction)
 - **WSRP/JPDK**: WSRP or Oracle JPDK portlet producer (before you create a resource of this type, register the associated producer as described in [Section 25.9, "Registering WSRP and Oracle JPDK Portlet Producers."](#))
 - **OpenSocial**: OpenSocial Container

Figure 25–6 Select Producer Type Dialog



4. Click **OK**. An entry called "<new>" will be added to the list of resources. This new resource will include the necessary configuration pages for the producer type chosen.
5. Configure the resource in the Pagelet Producer Console. The required configuration pages differ based on the type of producer. To save your changes at any time, click the **Save** icon in the navigator toolbar.
 - [Section 25.4.1, "Configuration Pages: Web and CSP Resources"](#)
 - [Section 25.4.2, "Configuration Pages for WSRP/JPDK Resources \(WSRP and Oracle JPDK Portlet Producers\)"](#)
 - [Section 25.4.3, "Configuration Pages for OpenSocial Resources \(OpenSocial Gadget Producers\)"](#)

Once the resource is defined, create pagelets and other objects within the resource.

- [Section 25.5, "Creating Pagelets"](#)
- [Section 25.6, "Creating Web Injectors"](#)
- [Section 25.7, "Creating Custom Parsers"](#)
- [Section 25.8, "Creating Hosted Files"](#)

25.4.1 Configuration Pages: Web and CSP Resources

The following configuration pages are used for Web and CSP resources:

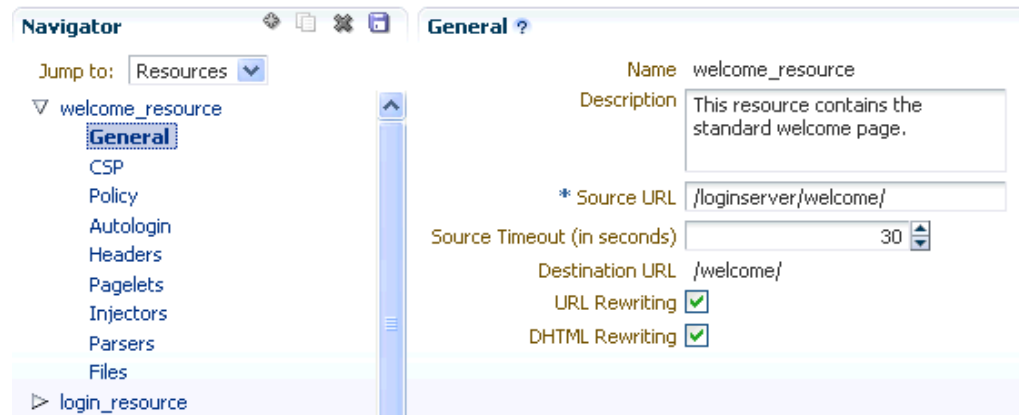
- [Section 25.4.1.1, "General"](#)
- [Section 25.4.1.2, "CSP"](#)
- [Section 25.4.1.3, "Policy"](#)
- [Section 25.4.1.4, "Autologin"](#)
- [Section 25.4.1.5, "Headers"](#)

This section uses the `welcome_resource` created when the Pagelet Producer is installed as an example.

25.4.1.1 General

On the **General** page, enter basic information about the resource.

Figure 25–7 Pagelet Producer Console: Resource - General Page



- Enter a **Name** for the resource.
- Enter a **Description** for the resource (optional).
- In the **Source URL** field, type the URL to the location of the web application resource to be proxied. For example, `http://internalServer/foo/`.

Note: If you are configuring an ADF Web Application as a resource, the Source URL cannot be any more specific than `http://hostname:portnumber/context-root/`.

- By default, the Pagelet Producer attempts to connect to the resource for 30 seconds before returning an error message. To change this value, enter a new **Source Timeout** period in seconds.
- In the **Destination URL** field, type the relative path to be used to access the resource. This path will be used to create an URL to the resource on the server that hosts the Pagelet Producer.
- The Pagelet Producer enables **URL Rewriting** by default. When URL rewriting is enabled, the Pagelet Producer rewrites URLs in the proxied application that begin with the source URL prefix so that they point to the destination URL prefix. If any

URLs point to other proxied CSP or web applications (also registered with the Pagelet Producer), those URLs will also be rewritten to use the proxy.

There are two cases in which you should disable URL rewriting:

- The internal URL prefix and external URL prefix are identical. In this case, the user's DNS must resolve the URL to the Pagelet Producer proxy server, and the Pagelet Producer proxy server's DNS must resolve the URL to the internal resource. Because DNS only resolves IP and not port, both servers must listen to the same port. This method is strongly recommended.
- All links in the application are relative URLs. In this case, the internal URL prefix path and the external URL prefix path must be identical. For example, if the internal URL prefix is `http://internal_server/bar/` the external URL prefix path must be `/bar/` or `http://proxy_server/bar/`.

To disable transformation, deselect **URL Rewriting**.

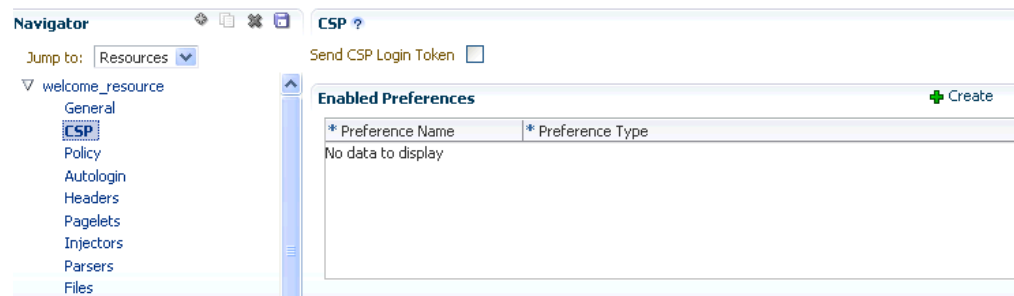
- To enable Dynamic HTML, choose **DHTML Rewriting**. This option supports URLs that are not in the original HTML returned from the server, but are added by DHTML. In most cases, this option should be enabled.

25.4.1.2 CSP

The preference headers specified on the CSP page are passed between the Pagelet Producer and remote CSP content producers. Basic preference types are supported natively and other preference types are mapped to one of the basic types.

Note: When accessing content that is built using web standards (javascript and HTML), these settings can be ignored or leveraged partially by sending the CSP-Set-Preference and CSP-Get-Preference headers as documented by the CSP protocol.

Figure 25–8 Pagelet Producer Console: Resource - CSP Page



User and session scope preferences can be shared by more than one pagelet. CSP metadata can be used to specify which session preferences can be set or obtained from the application and which user info preferences will be sent to the application. For example, if you store personally identifiable information such as an employee ID as a user preference, you can control which pagelets have access to this information.

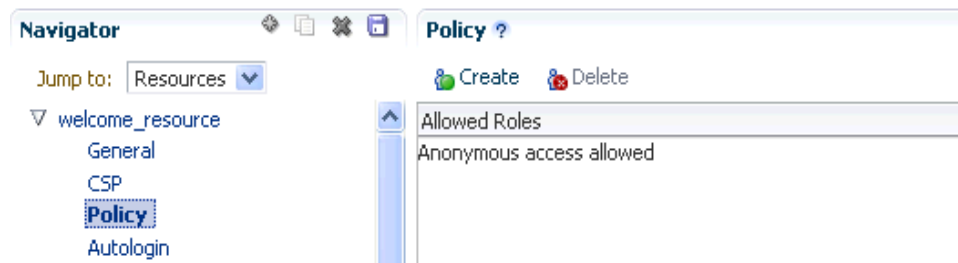
By default, the CSP login token is not passed to the proxied resource. To enable this feature, choose **Send CSP Login Token**. You must also enter the name and type of each of the settings that should be retrieved from the Pagelet Producer.

Note: Pagelets associated with a resource inherit this metadata.

25.4.1.3 Policy

The Policy page allows you to limit access to a resource to specific roles within Oracle WebCenter Portal.

Figure 25–9 Pagelet Producer Console: Resource - Policy Page



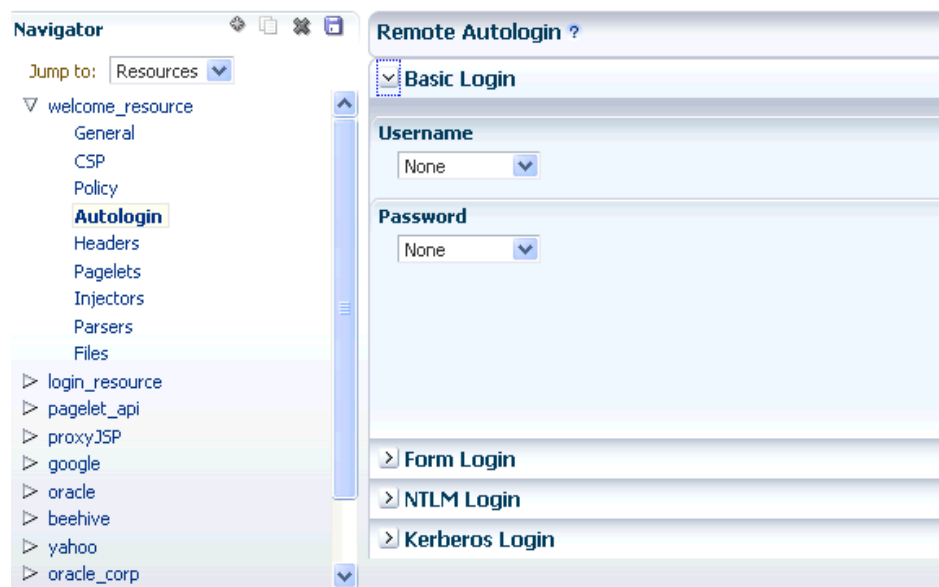
The J2EE container hosting the Pagelet Producer (such as Oracle WebLogic Server) is responsible for establishing the role memberships associated with the current user. A resource can specify multiple roles on the Policy page, and users will be allowed access if they are a member of any of the specified roles; otherwise they will be directed to a suitable J2EE container delegated authentication page to establish the required credentials. If no roles are entered in the list, anonymous access is allowed, and the resource is termed as an "anonymous resource".

Note: The role name(s) entered on this page must match those created in the J2EE container (such as Oracle WebLogic Server).

25.4.1.4 Autologin

The autologin feature allows the Pagelet Producer to supply credentials to applications automatically. The Autologin page allows you to configure authentication information for a resource for use by all users who access the resource.

Figure 25–10 Pagelet Producer Console: Resource - Autologin Page



The sections that follow describe how to configure credential mapping for authentication:

- [Section 25.4.1.4.1, "Form Login,"](#) describes how to configure autologin for a resource that prompts for authentication with an HTML form.
- [Section 25.4.1.4.2, "Basic Login and NTLM Login,"](#) describes how to configure autologin for a resource that prompts for authentication with basic authentication or NTLM.
- [Section 25.4.1.4.3, "Kerberos Login,"](#) describes how to configure autologin for a resource that prompts for authentication with Kerberos.
- [Section 25.4.1.4.4, "Authentication Sources,"](#) describes the static, user profile, and credential vault authentication field sources.

25.4.1.4.1 Form Login This section describes how to configure autologin for a resource that prompts for authentication with an HTML form.

1. On the **Autologin** page for the resource, expand the **Form Login** section.
2. The login page can be identified by an URL or a regular expression. In the **Login Form Identification** section, choose one of the following options:
 - If the login form is located at a static URL, select **URL** and type the URL into the box. You can choose to **Automatically Detect Form Fields** on the page or enter them manually as described in step 5 below.
 - If the login form is dynamic, select **RegEx** and type the regular expression pattern into the box.
3. Set the login form action. In the **Form Submit Location** section, choose one of the following options:
 - If the login form action is a static URL, select **URL** and type the URL into the box. Choose the action for the form submission: POST or GET.
 - If the login form is dynamic, select **RegEx** and type the regular expression pattern into the box.
4. To map fields from the form to authentication field sources, either click **Automatically Detect Form Fields** in the Login Form Identification section or enter them manually using the process below:
 - a. Click **Create** to add a new row to the **Form Fields** list.
 - b. Type the name of the HTML form input in the **Field Name** box.
 - c. For details on how to configure the **Source** and **Value** properties, see [Section 25.4.1.4.4, "Authentication Sources."](#)

Note: Sensitive fields should be stored securely using the credential vault (User Vault or Shared Vault).

- d. To delete field mappings, click **Delete**.
5. The logout page and login error pages can also be identified by an URL or a regular expression. In the **Logout Page Identification** and **Login Error Page Identification** sections, choose one of the following options:
 - If the page is located at a static URL, select **URL** and type the URL into the field provided.

- If the page is dynamic, select **RegEx** and type the regular expression pattern into the field provided.

25.4.1.4.2 Basic Login and NTLM Login This section describes how to configure autologin for a resource that prompts for authentication with basic authentication or NTLM.

1. On the **Autologin** page for the resource, expand the **Basic Login** or **NTLM Login** section.

Note: "Basic authentication transmits passwords as plain text, and therefore, it must not be used in production systems. Further, it is strongly recommended that the underlying transport is HTTPS."

2. In the **Username** and **Password** sections, choose the appropriate authentication source and enter a value as necessary. For details on how to configure these properties, see [Section 25.4.1.4.4, "Authentication Sources"](#).

25.4.1.4.3 Kerberos Login This section describes how to configure autologin for a resource that prompts for authentication using Kerberos. For information on defining basic Kerberos settings, see [Section 25.3, "Configuring Pagelet Producer Settings."](#)

1. On the **Autologin** page for the resource, expand the **Kerberos Login** section.
2. In the **Username** and **Password** sections, choose the appropriate authentication source and enter a value as necessary. For details on how to configure these properties, see the next section, [Section 25.4.1.4.4, "Authentication Sources"](#).
3. In the **SPN** field, enter the Service Principal Name (SPN) for the Kerberos account, in the format `http://hostname_with_kerberos`. (Before the Kerberos authentication service can use an SPN to authenticate a service, the SPN must be registered on the account object that the service instance uses to log on.)

25.4.1.4.4 Authentication Sources Authentication sources define the source for login fields. The following table describes each of the authentication field source values:

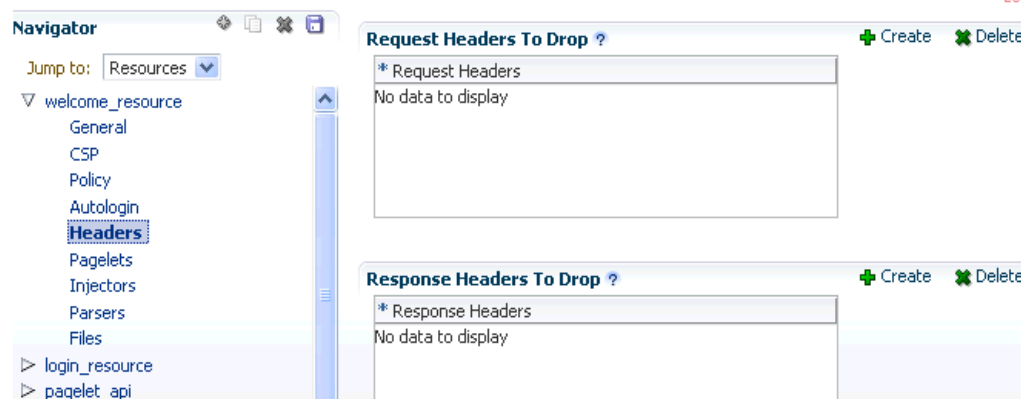
Table 25–2 Pagelet Producer Authentication Sources

Field	Description
Static	Uses the provided authentication information for all users accessing the resource. Type the static value in the field provided.
Profile	Uses properties from the user's Oracle WebCenter Portal profile to supply credential data for authentication.
User Vault or Shared Vault	<p>Prompts the user for credentials the first time the resource is accessed. The supplied credentials are encrypted and stored in the credential vault, and each subsequent access to the resource is authenticated with the stored credentials. When using vault storage, the key name chosen should be a generic placeholder and should not reflect sensitive information like the actual password.</p> <p>In the second field, enter the name of the credential vault to use, or leave the entry as "default" to use the server vault.</p> <p>User Vault stores one value per key per user, while Shared Vault stores one value per key for all users.</p>

25.4.1.5 Headers

The Headers page allows you to choose Request and Response headers that should be dropped from the HTTP that is provided by the Pagelet Producer.

Figure 25–11 Pagelet Producer Console: Resource - Headers Page



Some header elements should be blocked from being passed to back-end applications. For example, when using delegated (third-party SSO) authentication, the SSO system might insert some headers that need not be passed to the back-end applications. When passed, these headers might interfere with the back-end application functionality.

If any headers are specified on this page, only the specified headers will be dropped. If no headers are explicitly specified, the following headers are dropped by default:

Request Headers	Response Headers
- Cache-Control	- Max-Forwards
- Connection	- Proxy-Authenticate
- Cookie	- Proxy-Connection
- Host	- Set-Cookie
- Max-Forwards	- Trailer
- Pragma	- Transfer-Encoding
- Proxy-Connection	- Upgrade
- Proxy-Authorization	
- TE	
- Trailer	
- Transfer-Encoding	
- Upgrade	

To add a header to the list, click **Create** and enter the header name in the field provided. The Content-Length header is always implicitly dropped, because manipulating content during the proxying operation renders the content length invalid in almost all cases.

Once the resource is defined, you can create pagelets and other objects within the resource.

- [Section 25.5, "Creating Pagelets"](#)
- [Section 25.6, "Creating Web Injectors"](#)
- [Section 25.7, "Creating Custom Parsers"](#)
- [Section 25.8, "Creating Hosted Files"](#)

25.4.2 Configuration Pages for WSRP/JPDK Resources (WSRP and Oracle JPDK Portlet Producers)

The following configuration pages are used for WSRP/JPDK resources, which are based on WSRP or Oracle JPDK portlet producers.

Note: Before you can create a resource based on a WSRP or Oracle JPDK portlet producer, you must register the producer as described in [Section 25.9, "Registering WSRP and Oracle JPDK Portlet Producers."](#)

- [Section 25.4.2.1, "General"](#)
- [Section 25.4.2.2, "Policy"](#)

25.4.2.1 General

On the **General** page, enter basic information about the resource.

- Choose the portlet producer type from the **Portlet Producer** dropdown list. This list is populated with the producers that have been registered as described in [Section 25.9, "Registering WSRP and Oracle JPDK Portlet Producers."](#)
- Enter a **Name** for the resource.
- Enter a **Description** for the resource (optional).

25.4.2.2 Policy

The Policy page allows you to limit access to a resource to specific roles within Oracle WebCenter Portal.

The J2EE container hosting the Pagelet Producer (such as Oracle WebLogic Server) is responsible for establishing the role memberships associated with the current user. A resource can specify multiple roles on the Policy page, and users will be allowed access if they are a member of any of the specified roles; otherwise they will be directed to a suitable J2EE container delegated authentication page to establish the required credentials. If no roles are entered in the list, anonymous access is allowed, and the resource is termed as an "anonymous resource".

Note: The role name(s) entered on this page must match those created in the J2EE container (such as Oracle WebLogic Server).

Once the resource is defined, you can create pagelets and web injectors within the resource.

- [Section 25.5, "Creating Pagelets"](#)
- [Section 25.6, "Creating Web Injectors"](#)

25.4.3 Configuration Pages for OpenSocial Resources (OpenSocial Gadget Producers)

The following configuration pages are used for OpenSocial resources, which are based on OpenSocial gadget producers.

- [Section 25.4.3.1, "General"](#)
- [Section 25.4.3.2, "Policy"](#)

Note: Configure the Pagelet Producer for use with OpenSocial before creating an OpenSocial resource. For details, see [Section 25.3.6, "OpenSocial Settings."](#)

25.4.3.1 General

On the **General** page, enter basic information about the resource.

- Enter a **Name** for the resource.
- Enter a **Description** for the resource (optional).
- The **Source URL** field should be pre-filled with the relative URL to the internal OpenSocial Container ("/os/"). Registering external OpenSocial Containers is not supported.
- In the **Destination URL** field, type the relative path to be used to access the resource. This path will be used to create the URL to the OpenSocial container on the server that hosts the Pagelet Producer.

25.4.3.2 Policy

The Policy page allows you to limit access to a resource to specific roles within Oracle WebCenter Portal.

The J2EE container hosting the Pagelet Producer (such as Oracle WebLogic Server) is responsible for establishing the role memberships associated with the current user. A resource can specify multiple roles on the Policy page, and users will be allowed access if they are a member of any of the specified roles; otherwise they will be directed to a suitable J2EE container delegated authentication page to establish the required credentials. If no roles are entered in the list, anonymous access is allowed, and the resource is termed as an "anonymous resource".

Note: The role name(s) entered on this page must match those created in the J2EE container (such as Oracle WebLogic Server).

Once the resource is defined, you can create pagelets and files within the resource.

- [Section 25.5, "Creating Pagelets"](#)
- [Section 25.8, "Creating Hosted Files"](#)

25.5 Creating Pagelets

The pagelets collection lists the pagelets associated with the resource. To create a new pagelet, select the **Pagelets** section under the resource you want to use in the Pagelet Producer Console and click the **Create** icon in the toolbar. A pagelet called "<new>" will be added to the list. To modify an existing pagelet, click the pagelet name. Each pagelet has the following configuration pages:

- [Section 25.5.1, "General"](#)
- [Section 25.5.2, "Preferences"](#)
- [Section 25.5.3, "Parameters"](#)
- [Section 25.5.4, "Clipper"](#)
- [Section 25.5.5, "Documentation"](#)

25.5.1 General

Enter a **Name** for the pagelet and the **Library** name with which to associate the pagelet. (A pagelet library is a user-defined way to group related pagelets.) Enter a **Description** for the pagelet (optional).

The **Refresh Inline** option should be used only if the pagelet is to be injected into the page body without using an IFrame. Since IFrame injection is the default and recommended method for implementing partial page refresh for pagelet click-throughs, this option should only be enabled under very rare circumstances.

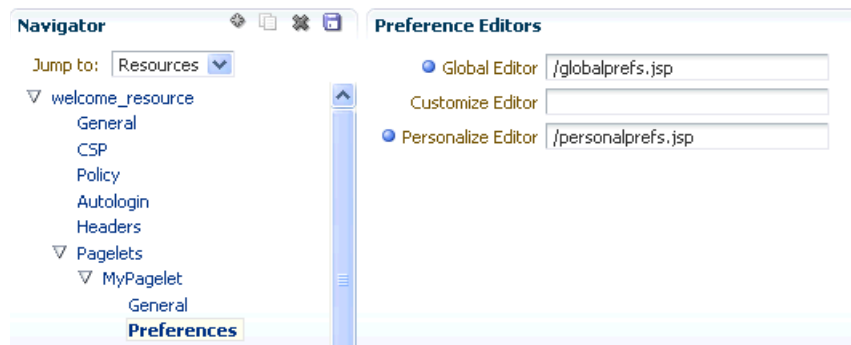
- **For web and CSP pagelets**, type the relative path to the pagelet in the **URL Suffix** field (do not include the Source URL prefix you entered for the resource). If you leave the URL Suffix blank, then the entire resource will be considered the pagelet.
- **For pagelets based on WSRP or Oracle JPDK portlets**, choose the portlet on which to base the pagelet from the **Portlet** dropdown list. This list is populated with the portlets on the WSRP or Oracle JPDK portlet producer associated with the parent resource. Any public parameters associated with the portlet will automatically be imported as pagelet parameters. For more information on working with WSRP and Oracle JPDK portlets, see [Section 25.9, "Registering WSRP and Oracle JPDK Portlet Producers"](#) and [Section 25.4.2, "Configuration Pages for WSRP/JPDK Resources \(WSRP and Oracle JPDK Portlet Producers\)."](#)
- **For pagelets based on OpenSocial gadgets**, enter the location of the gadget XML schema in the **Gadget URL** field. Click the **Import Gadget Metadata** button to import the following information from the XML schema:
 - **Gadget name**: This value will be imported into the Description field on the General page.
 - **Gadget user preferences**: The pagelet parameters on the [Parameters](#) page will be populated with the gadget's user preferences.
 - **Preference editor**: If there are any editable user preferences, the Personalize Editor field on the [Preferences](#) page will be populated and a preference page will be created using the preferences on the [Parameters](#) page.

25.5.2 Preferences

On the Preferences page, enter the relative URLs to any preference pages required by the pagelet: Global, Customize, or Personalize. Do not include the Source URL prefix you entered for the resource. (As noted above, for OpenSocial gadgets with user preferences, a default entry will be created; this entry should not be modified.)

The Preferences page is not used by WSRP or Oracle JPDK-based pagelets.

Figure 25–12 Pagelet Producer Console: Pagelets - Preferences Page



25.5.3 Parameters

Data can be passed to pagelets using pagelet parameters or the pagelet payload. Parameters pass name-value pairs to the pagelet application, while the payload is any text, including XML. You can write an XML Schema to describe the XML that a particular pagelet expects and document this by entering a URI to an XSD file or a namespace:name qualifier on this page. This value is for convenience only, it is not used or enforced at runtime.

On the Parameters page, enter the **Payload Schema** or the **Parameters** that should be passed to the pagelet.

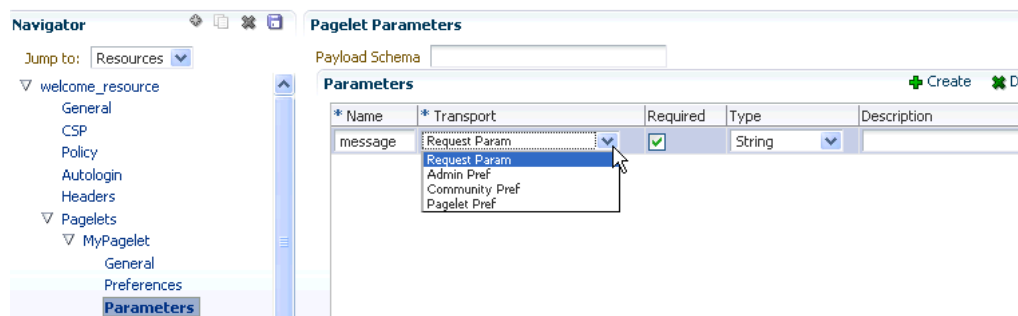
To add a parameter, click **Create**.

- Enter the **Name** of the parameter.
- Choose the **Transport** type: Request Parameter, Administrative Preference, Community Preference, or Pagelet Preference.

Note: The Request Parameter transport type should be used in most cases. Request Parameters are sent as query string arguments on the URL to the pagelet's host server. The preference transport types should only be used for CSP pagelets.

- If the parameter is required by the pagelet, select the **Required** checkbox.
- Choose the appropriate data **Type**: string or numeric.

Figure 25–13 Pagelet Producer Console: Pagelets - Parameters Page



25.5.4 Clipper

Clipping allows you to form a pagelet by clipping a portion of a larger web page in a proxied application. For example, in a news web page there is a box listing the latest headlines. By identifying the containing HTML for that box, you can clip only the headlines and serve that subset of the news web page as a pagelet.

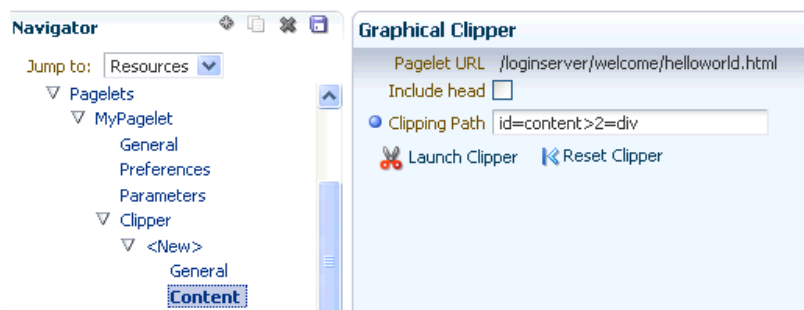
To create a clipper, select the **Clipper** section under the pagelet and click the **Create** icon in the toolbar. A new clipper will be created with two configuration pages:

- On the **General** page, enter a name for the clipper.
- On the **Content** page, define the clipper content.

In addition to clipping a portion of the body of the web page, the pagelet's <head> element can be included by choosing **Include head**. This allows CSS, JavaScript, or other declarations that occur in the <head> element to be included with the clipped body portion.

- To use a graphical tool to select page content, click **Launch Clipper**.
- To specify HTML tag attributes that describe the section to be clipped, expand the **Advanced Clipper** section and enter the tag name and associated attribute(s).

Figure 25–14 Pagelet Producer Console: Clipper - Content Page

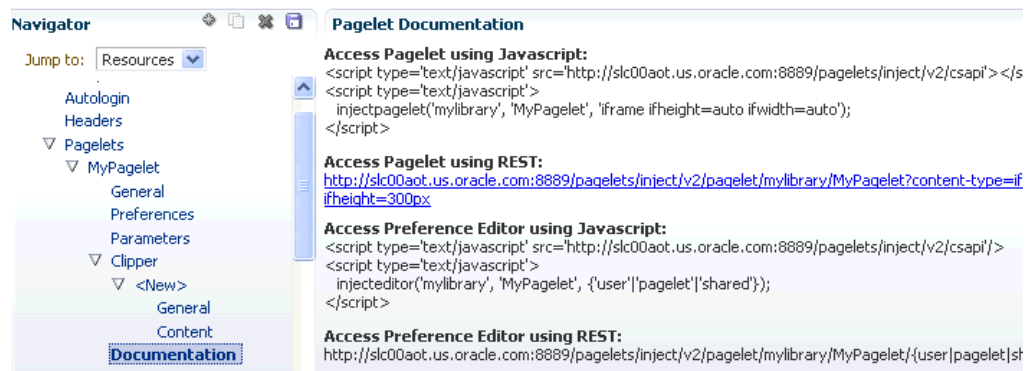


Keep the following in mind when using the clipper:

- If the back-end resource is accessed over HTTPS, make sure the Pagelet Producer Console is also accessed over a secure port.
- If the clip source is protected by a login form or other form of authentication, make sure to configure Autologin for the parent resource as described in [Section 25.4.1.4, "Autologin"](#). If you are using the vault to store credential values, make sure to capture the credentials prior to using the clipper.
- If you are having problems with the clipper, make sure the configured pagelet URL can be loaded by the browser without redirects. If necessary, change the pagelet suffix to reflect the final URL loaded by the browser after following all the redirects.
- Images and code overwritten using hosted files cannot be clipped. (For details on hosted files, see [Section 25.8, "Creating Hosted Files."](#))

25.5.5 Documentation

The Documentation page displays sample code to access the pagelet and preference editor using either the JavaScript or REST API.

Figure 25–15 Pagelet Producer Console: Pagelets - Documentation Page

25.6 Creating Web Injectors

A web injector inserts content into a specified location in the proxied resource page. The content may be any text, including HTML, CSS, JavaScript, and pagelet declarations. An empty injector may also be used to remove unwanted content from a page. Injectors cannot be created for OpenSocial resources.

To create a web injector, select the **Injectors** section under the resource you want to use and click the **Create** icon in the toolbar. A new injector called "<new>" will be added to the list. Injectors have the following configuration pages:

- [Section 25.6.1, "General"](#)
- [Section 25.6.2, "Content"](#)

25.6.1 General

Enter a **Name** for the web injector.

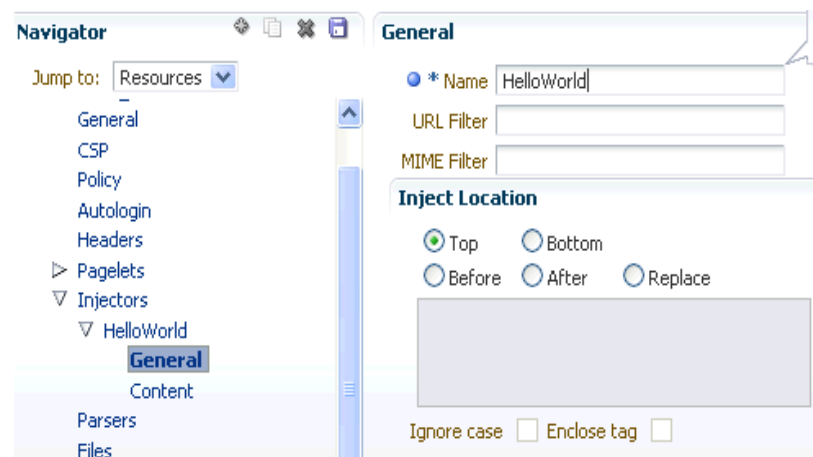
The injector can be applied to a subset of the resource by typing a URL pattern into the **URL Filter** box. The injector will be applied only to those URLs within the resource that begin with the text in the URL Filter box. If the box is empty or contains only a '/', the injector will be applied to the entire resource.

To restrict the injector to specific kinds of content, type a comma separated list of MIME types in the **MIME Filter** box. For example, *text/html* restricts the injector to HTML content, while *text/css* only restricts the injector to CSS content.

Define where in the resource's output the injection will be made:

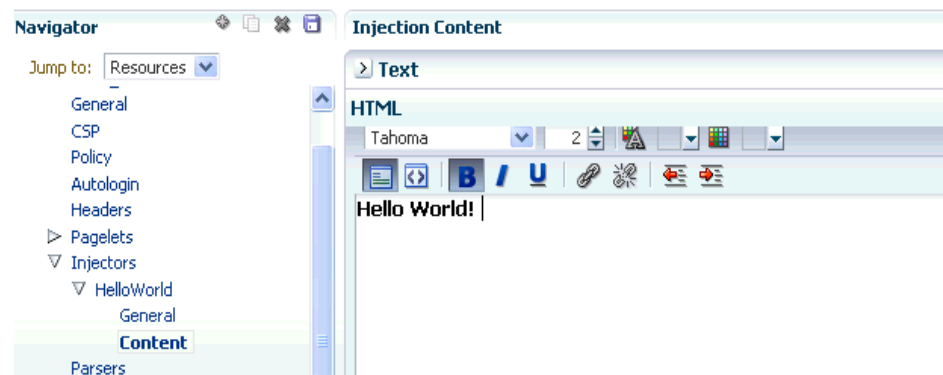
- **Top** puts the content first in the page. Do not use this option to inject pagelet declarations.
- **Bottom** puts the content last in the page.
- The **Before/After/Replace** options put the content into the page relative to the unique string specified in the field provided. You can choose to ignore the case of the string by selecting **Ignore case**.

The **Enclose tag** option identifies the unique string and replaces both the text and the enclosing tag with the content specified on the next page.

Figure 25–16 Pagelet Producer Console: Injectors - General Page

25.6.2 Content

Content to be injected may be any text, including HTML, CSS, JavaScript, and pagelet declarations. Content can be entered using the text editor or the HTML editor.

Figure 25–17 Pagelet Producer Console: Injectors - Content Page

25.7 Creating Custom Parsers

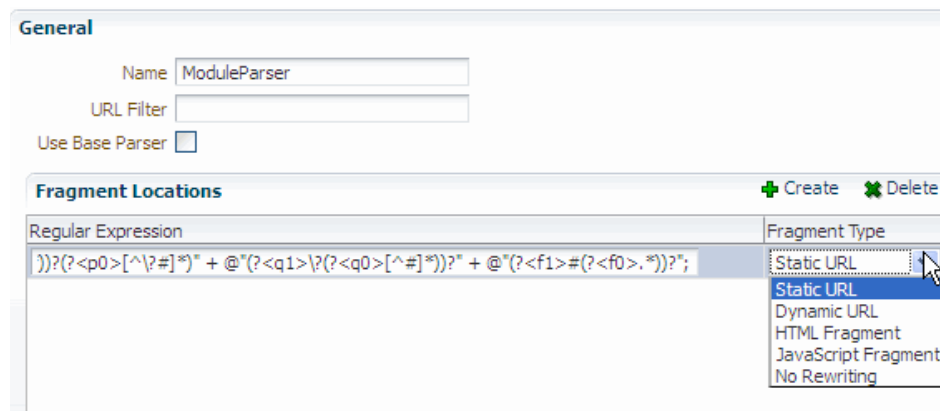
Custom parsers allow you to supplement or change built-in logic for parsing content and finding URLs. When the built-in parsers fail to identify URLs or identify sections that must not be rewritten as URLs, custom parsers can be used to change the default behavior. Parsers cannot be created for WSRP or Oracle JPKD portlet producers or OpenSocial gadget producers.

To create a custom parser, select the **Parsers** section under the resource you want to use and click the **Create** icon in the toolbar.

- Enter a **Name** for the parser.
- The parser can be applied to a subset of the resource by typing a URL pattern into the **URL Filter** box. The parser will be applied only to those URLs within the resource that begin with the text in the URL Filter box. If the box is empty or contains only a '/', the parser will be applied to the entire resource.

- To add a new parsing rule, click **Create** to add a new row to the **Fragment Locations** section.
- In the **Regular Expressions** column, enter the regular expression for identifying the URL fragment that should be transformed. The first grouping expression (in parentheses) identifies the fragment, and the rest of the expression provides the context for finding it.
- Choose the **Fragment Type** to define how the selected location should be parsed:
 - **Static URLs** are transformed on the server.
 - **Dynamic URLs** are transformed using JavaScript on the client.
 - **HTML Fragment** and **Javascript Fragment** types are used for content that is embedded in another content type, such as XML.
 - **No Rewriting** specifies a location that should not be searched for URLs. This option is used to prevent rewriting of markup mistakenly identified as URLs.
- Click the **Save** icon in the navigator toolbar.

Figure 25–18 Pagelet Producer Console: Parsers - General Page



25.8 Creating Hosted Files

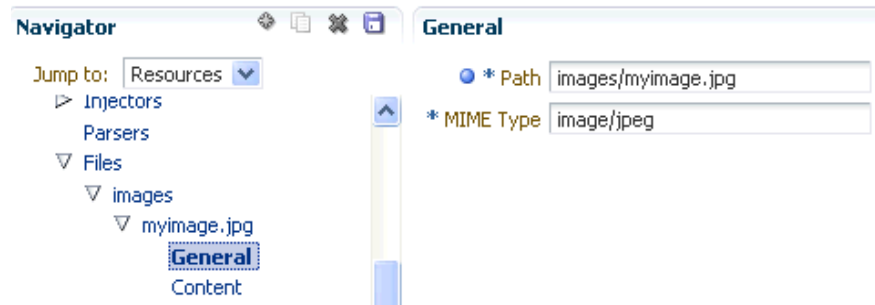
The Pagelet Producer can host all types of content (HTML, JavaScript, CSS, etc.) and present the file at a virtual URL location. Hosted files can be used for a range of purposes:

- Overwrite content and functionality in a proxied application, by uploading files and configuring them to use the same URL as the original file.
- Use hosted files in injectors to insert images or content into a proxied application.
- Host pagelet files on the Pagelet Producer server.

To upload a file, select the **Files** section under the resource you want to use and click the **Create** icon in the toolbar.

- On the **General** page, enter the relative path to the file in the **Name** field. Do not use a leading forward-slash ("/"). The directory structure of the Files collection in the navigator is updated to match the path to the file.

Enter the **MIME type** of the file.

Figure 25–19 Pagelet Producer Console: Files - General Page

- On the **Content** page, enter the path to the file or click the Browse button to navigate to the file.

Click the **Upload** button to upload the file to the Pagelet Producer server. If you entered text or html as the MIME type, you can also use the editor on the Content page to enter or edit file content. (The editor is only available for text and html files.) If you entered an image type as the MIME type, the uploaded image will be displayed on the Content page.

Note: Text files (text/plain) uploaded to the Pagelet Producer must be saved as UTF-8.

- Click the **Save** icon in the navigator toolbar.

After the file is uploaded, it will be available for use in injectors and pagelets at the following URL:

```
http://<host_name>:<port_number>/pagelets/<resourcename>/<filepath>
```

For example, if the file was uploaded under the "welcome_resource" resource and the name for the file was entered as "images/myimage.jpg" the path to the hosted file on the Pagelet Producer server would be:

```
http://<host_name>:<port_number>/pagelets/welcome_resource/images/myimage.jpg
```

Keep the following in mind when working with hosted files:

- The hosted file feature should not be used for bulky files.
- If you choose to host OpenSocial gadget XML files, the files must be placed under an anonymous resource (with no security policy) or gadget functionality will not work correctly.
- Hosted files cannot be created for WSRP or Oracle JPDK portlet producers.

25.9 Registering WSRP and Oracle JPDK Portlet Producers

The Pagelet Producer can expose WSRP and Oracle JPDK portlets as pagelets for use in Framework applications, Spaces, and third-party portals. After registration, the associated resource in the Pagelet Producer is automatically populated with pagelets to represent the portlets associated with the portlet producer.

This section provides detailed instructions on registering WSRP and Oracle JPDK portlet producers and importing the associated portlets.

- [Section 25.9.1, "Registering WSRP Portlet Producers"](#)
- [Section 25.9.2, "Registering Oracle JPDK Portlet Producers"](#)
- [Section 25.9.3, "Using WSRP and Oracle JPDK Portlets"](#)

Note: By default, access to producer registration is limited to Oracle WebLogic Server Administrators.

If a user should have access and it is not possible to add the user to the Administrators group; use the `grantAppRole` WLST command as shown below:

```
grantAppRole (appStripe="pagelet-producer" ,
> appRoleName="AppConnectionManager" ,
> principalClass="weblogic.security.principal.WLSUserImpl" ,
> principalName="monty")
```

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

25.9.1 Registering WSRP Portlet Producers

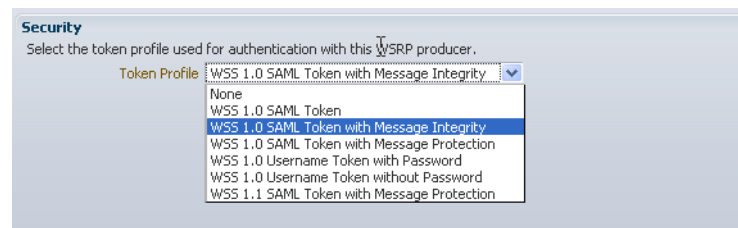
You can use Enterprise Manager, WLST or the Pagelet Producer Console to register a WSRP endpoint as a portlet producer. After registration, a new Pagelet Producer resource is created and automatically populated with pagelets to represent the portlets associated with the WSRP endpoint.

1. Register the WSRP endpoint using either Enterprise Manager or the Pagelet Producer Console.
 - In Enterprise Manager, go to the Pagelet Producer application. From the Application Deployment menu, click **WebCenter Portal > Register Producer**.
 - In the Pagelet Producer Console, choose **Producers** from the dropdown menu in the navigator toolbar. On the Portlet Producer page, click **Register**.
2. Enter a name for the producer. Choose **WSRP Producer** as the **Producer Type**.
3. Enter the **WSDL URL** for the WSRP endpoint (for example, `http://www.oasis-open.org/committees/wsrp/specifications/version1/wsrp_v1_interfaces.wsdl`).

Figure 25–20 Pagelet Producer Console: Register Portlet Producer - WSRP Producer

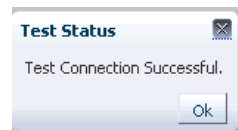
4. If an HTTP proxy is required when contacting the producer, select the **Use Proxy?** option and enter the host name and port number for the proxy server. (A proxy is required if the Pagelet Producer and the portlet producer are separated by a firewall)
5. Enter a suitable **Default Execution Timeout** for communications with the producer. The default is 30 seconds. Individual portlets may define their own timeout period, which takes precedence over the value defined here.
6. If the producer requires authentication, select the appropriate **Token Profile** from the dropdown list in the **Security** section and enter any necessary configuration information. If a keystore is used by the selected token profile, the path to the keystore entered on this page must be absolute.

Figure 25–21 Pagelet Producer Console: Register Portlet Producer - WSRP Producer: Token Profile



7. Click the **Save** icon in the navigator toolbar.
8. To confirm that the configuration is correct, click the **Test** button.

Figure 25–22 Pagelet Producer Console: Register Portlet Producer - Successful Test Popup



If the test is successful, click **OK** to close the popup. If the test is not successful, click **OK** to close the popup and make modifications to the configuration as necessary.

9. After you have run a test successfully, click **OK** to save your configuration settings and return to the Portlet Producers list.
10. If you registered the producer in Enterprise Manager, you must load the external registration in Pagelet Producer. Either restart the Pagelet Producer server, or complete the following steps:
 - a. Open the Pagelet Producer Console and select **Producers** from the drop-down list in the navigator toolbar.
 - b. On the Portlet Producers page, select the new WSRP producer and click **Refresh**.

Once registration is complete, the WSRP producer will appear as a resource in the Pagelet Producer Console, and the portlets associated with the WSRP endpoint will be listed in the pagelets collection for the resource.

The settings and parameters for the new pagelets are based on the portlet definitions in the WSDL for the WSRP producer. If additions or modifications are made to the WSRP portlets, refresh the producer registration as described in step 10 above to import the changes. WSRP-based pagelets can be used like any other pagelets.

Note: Auto-generated resources and pagelets cannot be modified. To make changes to the WSRP-based pagelets, follow the steps in the next section, [Section 25.9.3, "Using WSRP and Oracle JPDK Portlets."](#)

25.9.2 Registering Oracle JPDK Portlet Producers

Oracle WebCenter Portal's Pagelet Producer can expose Oracle JPDK portlets as pagelets for use in Framework applications, Spaces, and third-party portals.

You can use Enterprise Manager, WLST or the Pagelet Producer Console to register a Oracle JPDK endpoint as a portlet producer. After registration, a new Pagelet Producer resource is created and automatically populated with pagelets to represent the portlets associated with the Oracle JPDK producer.

1. Register the Oracle JPDK endpoint using either Enterprise Manager or the Pagelet Producer Console.
 - In Enterprise Manager, go to the Pagelet Producer application. From the Application Deployment menu, click **WebCenter Portal > Register Producer**.
 - In the Pagelet Producer Console, choose **Producers** from the dropdown menu in the navigator toolbar. On the Portlet Producer page, click **Register**.
2. Enter a name. Choose **Oracle PDK-Java Producer** as the **Producer Type**.
3. Enter the **URL Endpoint** for the Oracle JPDK producer using the following syntax: `http://host_name:port_number/context_root/providers` where `host_name` is the server where the producer is deployed, `port_number` is the HTTP Listener port number and `context_root` is the application's context root (`providers` is static text). For example: `http://myHost.com:7778/myEnterprisePortlets/providers`.

Figure 25–23 Pagelet Producer Console: Register Portlet Producer Page - Oracle PDK-Java Producer

The screenshot shows the 'Register Portlet Producer' page in the Pagelet Producer Console. At the top, there is a 'Navigator' section with a 'Jump to:' dropdown menu set to 'Producers'. To the right are 'Test', 'Ok', and 'Cancel' buttons. The main form is titled 'Register Portlet Producer' and is divided into several sections:

- Name And Type:** Contains a text field for 'Producer Name' with the value 'jpd_k_producer' and a radio button selection for 'Producer Type' with 'Oracle PDK-Java Producer' selected.
- Portlet Producer URL:** Contains a text field for 'URL Endpoint' with the value 'http://myHost.com:7778/myEnterprisePortlets/providers'. Below this are fields for 'Service ID', 'Use' (checkbox), 'Proxy?' (checkbox), 'Proxy Host', 'Proxy Port', 'Associated External Application' (dropdown), and 'Establish Session?' (checkbox).
- Advanced Configuration:** Contains a heading 'Specify additional (optional) information.' and three text input fields: 'Default Execution Timeout (Seconds)', 'Subscriber ID', and 'Shared Key'.

4. If an HTTP proxy is required when contacting the producer, select the **Use Proxy?** option and enter the host name and port number for the proxy server. (A proxy is required if the Pagelet Producer and the portlet producer are separated by a firewall).
5. If any of the portlets on the Oracle JPKD producer require authentication, select the relevant external application from the **Associated External Application** drop-down list.
6. To enable a user session when executing portlets from the Oracle JPKD producer, select the **Establish Session?** option. Sessions are maintained on the producer server, allowing portlet code to maintain information in the session. Message authentication uses sessions, so if a shared key is specified in the Advanced Configuration section, this option should also be selected. For sessionless communication between the producer and the server, do not select this option.
7. Enter a suitable **Default Execution Timeout** for communications with the producer (the maximum time the producer may take to register, deregister, or display portlets). The default is 30 seconds. Individual portlets may define their own timeout period, which takes precedence over the value defined here.
8. In the **Subscriber ID** field, enter a string to identify the consumer of the producer being registered. When a producer is registered with an application, a call is made to the producer. During the call, the consumer 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.
9. If the producer is set up to handle encryption, enter a **Shared Key** (also known as the HMAC key). 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 value here. The shared key can contain between 10 and 20 alphanumeric characters.
10. Click the **Save** icon in the navigator toolbar.
11. To confirm that the configuration is correct, click the **Test** button.

Figure 25–24 Pagelet Producer Console: Register Portlet Producer - Successful Test Popup



If the test is successful, click **OK** to close the popup. If the test is not successful, make modifications to the configuration as necessary and run the test again.

12. After you have run a test successfully, click **OK** to save your configuration settings and return to the Portlet Producers list.
13. If you registered the producer in Enterprise Manager, you must load the external registration in Pagelet Producer. Either restart the Pagelet Producer server, or complete the following steps:
 - a. Open the Pagelet Producer Console and select **Producers** from the drop-down list in the navigator toolbar.
 - b. On the Portlet Producers page, select the new Oracle JPKD producer and click **Refresh**.

Once registration is complete, the Oracle JPDK producer will appear as a resource in the Pagelet Producer Console, and the portlets associated with the producer will be listed in the pagelets collection for the resource.

The settings and parameters for the new pagelets are based on the portlet definitions in the producer URL. If additions or modifications are made to the portlets, refresh the producer registration as described in step 13 above.

Note: Auto-generated resources and pagelets cannot be modified. To make changes to the Oracle JPDK-based pagelets, see the next section, [Section 25.9.3, "Using WSRP and Oracle JPDK Portlets."](#)

25.9.3 Using WSRP and Oracle JPDK Portlets

Auto-generated WSRP and Oracle JPDK resources and pagelets cannot be modified. Primarily intended for initial testing, they are virtual entries and do not exist in Pagelet Producer metadata definitions.

To make changes and create a permanent reference to the producer, the auto-generated resource must be cloned. To create a version that can be modified, choose the resource in the Pagelet Producer Console navigator and click **Clone**. The cloned version of the resource can be edited, and various elements such as injectors can be added to customize pagelet functionality. Cloned resources are stable and will be included in metadata exports.

You can also define a portlet-based pagelet from scratch by creating a new resource based on an existing portlet producer and then creating individual pagelets. For details, see [Section 25.4, "Creating Resources."](#)

25.10 Troubleshooting

Keep the following common configuration errors in mind when troubleshooting resources and pagelets. For details on configuring Pagelet Producer settings, see [Section 25.3, "Configuring Pagelet Producer Settings."](#)

- If you are using SSL, make sure both HTTP (nonsecure) and HTTPS (secure) ports are configured properly on the Transform page of the Pagelet Producer settings.
- If you are proxying external sites on a network that requires an HTTP proxy, you must configure the proxy URL on the Proxy page of the Pagelet Producer settings.
- Confirm that the `login_resource` and `pagelet_api` resources, created by default, are present and correctly configured.
- If you are proxying KD Browser or other CSP pagelets, make sure the image service URL is absolute and the CSP SOAP API URL is set correctly in the CSP page of the Pagelet Producer settings.
- Due to restrictions in the Sun Java Virtual Machine (JVM), pagelets cannot use HTTPS content where the underlying certificate uses MD2 signing algorithm.

For additional troubleshooting information, use logging. The Pagelet Producer logs messages to the standard Oracle Diagnostic Logging facility. In Oracle WebLogic Server, that location is: `user-projects/domains/<domain>/servers/<server>/logs/<server>-diagnostic.log`. For details on configuring logging, see [Section 25.3.1, "Logging Settings."](#) For more information on debugging pagelets, see *Creating Pagelets with Oracle WebCenter Portal's Pagelet Producer* in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*

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 Portal application's single sign-on process.

System administrators can use Fusion Middleware Control or the WLST command-line tool to register and manage external applications for WebCenter Portal application deployments.

Application administrators can also register and manage external applications at runtime through out-of-the-box administration pages or using external application task flows.

All external application changes that you make for WebCenter Portal applications, post deployment, are stored in the MDS repository as customizations.

Note: External application configuration is dynamic. Configuration changes are immediately reflected in the WebCenter Portal application; it is not necessary to restart the application or the managed server.

This chapter includes the following sections:

- [Section 26.1, "What You Should Know About External Applications"](#)
- [Section 26.2, "Registering External Applications"](#)
- [Section 26.3, "Modifying External Application Connection Details"](#)
- [Section 26.4, "Testing External Application Connections"](#)
- [Section 26.5, "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."](#)

26.1 What You Should Know About External Applications

If your WebCenter Portal application (Framework application or Spaces 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 user name and password, and any other credentials for the external application, and supplies it to the WebCenter Portal services or application requiring the credentials. The WebCenter Portal 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 Portal 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.

Note: When logging in to an external application, if you clear the **Remember My Login Information** check box, then the credentials provisioned for that user session are lost in the event of a failover in a high availability (HA) environment. You are prompted to specify the credentials again if you try to access the external application content in the same user session.

The external applications that are to be used by a Framework application can be specified before deployment through a wizard in Oracle JDeveloper, or after deployment through Fusion Middleware Control Console ([Figure 26-1](#)) or using WLST commands. Post-deployment, external applications specified at design time in JDeveloper display automatically. However, after deployment you must reprovision design-time shared and public credentials using Fusion Middleware Control or WLST commands. For information, see [Chapter 29, "Configuring the Identity Store,"](#) and [Chapter 30, "Configuring the Policy and Credential Store."](#)

Note: In Spaces, you can register external applications using the External Application task flow available by default, or you can add a task flow to register and manage your applications. For information about registering external applications using External Application task flows in Spaces, see the sections "Registering External Applications Through Spaces Administration" and "Working with the External Application Task Flow" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

Figure 26–1 Edit External Application

Edit External Application Connection ? OK Cancel

Name

Application Name MS-Exchange
 Display Name

Login Details
 View the HTML source of the application's login form to determine the Login URL and field names for the HTML User ID and User Password

Enable Automatic Login

* Login URL

* HTML User ID Field Name

* HTML User Password Field Name

Authentication Details
 The authentication method specifies how message data is sent by the browser. View the HTML source of the application's login form to determine the method used, for example, <form method="POST">.

Authentication Method

Additional Login Fields

Shared Credentials
 When shared credentials are enabled, authenticated WebCenter users log in to the application using the user name and password defined here. WebCenter users are not presented with a login form.

Enable Shared Credentials

User Name

Password

Public Credentials
 When public credentials are enabled, unauthenticated WebCenter users (public users) log in to the application using the user name and password defined here. WebCenter users are not presented with a login form.

Enable Public Credentials

User Name

Password

26.2 Registering External Applications

You can register external applications for WebCenter Portal 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 Portal 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	https://login.yahoo.com/config/login?/login?	action
User Name / User ID Field	login	name="login"
Password Field Name:	passwd	name="passwd"
Authentication Method	post	method

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 Portal application.

For information about services that use external applications, see the section "Secured Service Connections" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

This section includes the steps for:

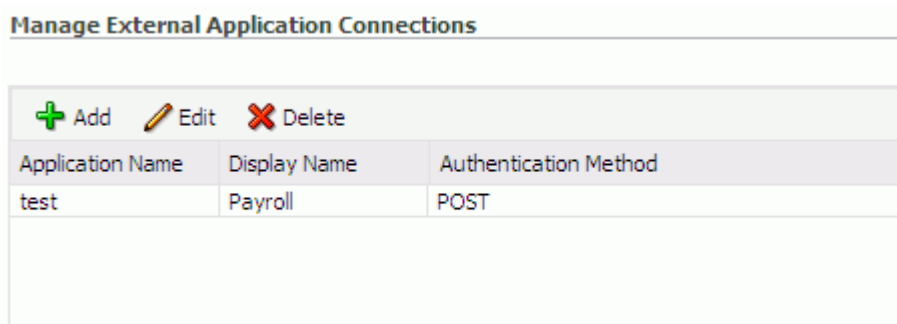
- [Section 26.2.1, "Registering External Applications Using Fusion Middleware Control"](#)
- [Section 26.2.2, "Registering External Applications Using WLST"](#)
- [Section 26.2.3, "Registering External Applications in the Spaces Application"](#)
- [Section 26.2.4, "Registering External Applications in Framework Applications"](#)

26.2.1 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 Portal application (Framework application or Spaces application):
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
2. Do one of the following:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
3. From the list of services on the **WebCenter Portal Service Configuration** page, choose **External Applications**.
4. To register a new external application, click **Add** ([Figure 26–2](#)).

Figure 26–2 Configuring External Application Connections



5. Enter a unique name for the external application and a display name that WebCenter Portal users working with this external application will see.

See also [Table 26–1](#).

Table 26–1 External Application Connection - Name

Field	Description
Application Name	<p>Enter a name for the application. The name must be unique (across all connection types) within the WebCenter Portal application.</p> <p>For example: yahoo</p> <p>Note: Once registered, you cannot edit the Application Name.</p>
Display Name	<p>Enter a user friendly name for the application that WebCenter Portal users will recognize. WebCenter Portal end-users working with this external application will see the display name you specify here.</p> <p>For example: My Yahoo</p> <p>If you leave this field blank, the Application Name is used.</p>

6. Enter login details for the external application.

For details, see [Table 26–2](#).

Table 26–2 External Application Connection - Login Details

Field	Description
Enable Automatic Login	<p>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</p> <p>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.</p> <p>Note: Automated login is not supported for:</p> <ul style="list-style-type: none"> ■ External applications using BASIC authentication. ■ External applications configured for SSO. ■ External applications with a customized login form (built using ADF Faces) that does not implement the J2EE security container login method <code>j_security_check</code> for authentication. ■ External sites that do not support UTF8 encoding. ■ External applications that accept randomly generated hidden field values or cookies for successful login.
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>Note: 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.</p>

Table 26–2 (Cont.) External Application Connection - Login Details

Field	Description
HTML User ID Field Name	<p>Enter the name that identifies the "user name" or "user ID" field on the login form.</p> <p>Tip: To find this name, look at the HTML source for the login page.</p> <p>This property does not specify user credentials.</p> <p>Mandatory if the Authentication Method is GET or POST. Leave this field blank if the application uses BASIC authentication (see Authentication Method).</p>
HTML User Password Field Name	<p>Enter the name that identifies the "password" field on the login form.</p> <p>Tip: To find this name, look at the HTML source for the login page.</p> <p>Mandatory if the Authentication Method is GET or POST. Leave this field blank if the application uses BASIC authentication (see Authentication Method).</p>

7. Select the authentication method used by the external application.

For details, see [Table 26–3](#).

Table 26–3 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"> ■ GET: 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. ■ POST: Submits login credentials within the body of the form. This is the default. ■ BASIC: 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. <p>The Authentication Method 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><form method="POST" action="https://login.yahoo.com/config/login?" AutoComplete="off"></code></p>

8. Specify additional login fields and details, if required.

For details, see [Table 26–4, "External Application Connection - Additional Login Fields"](#).

Table 26–4 External Application Connection - Additional Login Fields

Field	Description
Additional Login Fields	<p>If your application requires additional login criteria, expand Additional Login Fields.</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 Add to specify an additional field for the login form. For each new field, do the following:</p> <ul style="list-style-type: none"> ■ Name - 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. ■ Value - 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. ■ Display to User - Select to display the field on the external application login screen. If the field is not displayed (unchecked), then a default Value must be specified. <p>Click Delete to remove a login field.</p>

9. Specify shared and public user credentials, if required.

For details, see [Table 26–5](#).

Table 26–5 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 Enable Shared Credentials, and then enter User Name and Password credentials for the shared user.</p> <p>When shared credentials are specified, every user accessing this external application, through the WebCenter Portal application, is authenticated using the user name and password defined here. WebCenter Portal users are not presented with a login form.</p> <p>Because WebCenter Portal 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>.</p> <p>See also "Providing Login Information for External Applications" in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces</i>.</p>
Enable Public Credentials	<p>Indicate whether unauthenticated users (public users) may access this external application. Select Enable Public Credentials, and then enter User Name and Password credentials for the public user.</p> <p>When public credentials are specified, public users accessing this external application through the WebCenter Portal 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.

26.2.2 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 `addExtAppCredential` to add shared or public credentials for an existing external application connection. For details, see `addExtAppCredential` 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 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

26.2.3 Registering External Applications in the Spaces Application

For information about registering external applications in the Spaces application, see the section "Registering External Applications Through Spaces Administration" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

26.2.4 Registering External Applications in Framework Applications

For information about registering external applications in Framework applications, see section "Managing External Applications" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

26.3 Modifying External Application Connection Details

This section shows you how to modify the external application connection details by:

- [Section 26.3.1, "Modifying External Application Connection Using Fusion Middleware Control"](#)
- [Section 26.3.2, "Modifying External Application Connection Using WLST"](#)

26.3.1 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 Framework application (or Spaces application):
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#).
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
2. Do one of the following:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
3. From the list of services on the **WebCenter Portal 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 26–2](#).

Note that you cannot edit the name of the external application.

6. Click **OK** to save your changes.

26.3.2 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 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

For information about modifying external applications in Spaces, see the section "Editing External Application Connection Details" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

26.4 Testing External Application Connections

For external applications that are created using login URLs, ensure that their login URLs are accessible. For information about direct URLs, see the section "Automated Single Sign-On" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

26.5 Deleting External Application Connections

Take care when deleting an external application connection as WebCenter Portal application users will no longer have access to that application, and any services dependent on the external application may not function correctly.

In Spaces, links to external applications are not automatically removed from the Application Navigator task flow when an external application is deleted. To prevent unsuccessful access attempts, administrators are advised to remove links to unavailable applications.

This section includes the following subsections:

- [Section 26.5.1, "Deleting External Application Connections Using Fusion Middleware Control"](#)
- [Section 26.5.2, "Deleting External Application Connections Using WLST"](#)
- [Section 26.5.3, "Deleting External Applications Connections in WebCenter Portal: Spaces"](#)

26.5.1 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 Framework application (or Spaces application):
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#).
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
2. Do one of the following:
 - For the Spaces application - From the **WebCenter Portal** menu, choose **Settings > Service Configuration**.
 - For Framework applications - From the **Application Deployment** menu, choose **WebCenter Portal > Service Configuration**.
3. From the list of services on the **WebCenter Portal Service Configuration** page, choose **External Applications**.
4. Select the name of the external application you want to remove, and click **Delete**.

26.5.2 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 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

26.5.3 Deleting External Applications Connections in WebCenter Portal: Spaces

For information about deleting external applications in Spaces, see the section "Deleting External Applications" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

26.5.4 Deleting External Applications Connections in WebCenter Portal: Framework Applications

For information about deleting external applications in Framework applications, see the section "Deleting External Application Registration Details in Oracle JDeveloper" in *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

Managing REST Services

This chapter provides an overview of managing Oracle WebCenter Portal's REST services in WebCenter Portal applications.

This chapter includes the following sections:

- [Section 27.1, "What You Should Know About REST Services"](#)
- [Section 27.2, "Performing Required Manual Configurations to Enable REST"](#)
- [Section 27.3, "Understanding Security Tokens"](#)
- [Section 27.4, "Configuring a Proxy Server"](#)
- [Section 27.5, "Changing the REST Root Name"](#)
- [Section 27.6, "Using Compression"](#)
- [Section 27.7, "Handling Authentication"](#)

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). For more information, see [Section 1.8, "Understanding Administrative Operations, Roles, and Tools."](#)

27.1 What You Should Know About REST Services

REST (REpresentational State Transfer) is an architectural style for making distributed resources available through a uniform interface that includes uniform resource identifiers (URIs), well-defined operations, hypermedia links, and a constrained set of media types. Typically, these operations include reading, writing, editing, and removing. Media types include JSON and XML/ATOM.

REST APIs are commonly used in client-side scripted, Rich Internet Applications. For example, a browser-based application written in Javascript can use Ajax techniques with REST APIs to send and receive application data from the server and update the client view.

WebCenter Portal provides a RESTful interface to many of its services, like Discussions, Lists, People Connections, and Search. For a complete list of the services that support REST, see "Using Oracle WebCenter Portal REST APIs" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

For a more complete introduction to REST and the WebCenter Portal REST APIs, see "Using Oracle WebCenter REST APIs" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

27.2 Performing Required Manual Configurations to Enable REST

The WebCenter Portal REST APIs are not enabled by default. To enable the REST APIs to work, you must perform a manual configuration procedure. This procedure prepares the credential store to handle encrypted security tokens.

For detailed information on the required configuration steps see [Section 20.2, "Before You Begin: Performing Required Configurations."](#)

27.3 Understanding Security Tokens

A user-scoped security token is embedded in the `href` and `template` attributes of every REST service URI. The token is both generated and validated by the server. The purpose of the security token is to prevent Cross-Site Request Forgery (CSRF) attacks.

For example:

```
<link
  template="opaque-template-uri/@me?startIndex={startIndex}
    &itemsPerPage={itemsPerPage}&token=generated-token"
  resourceType="urn:oracle:webcenter:messageBoard"
  href="opaque-uri/@me?token=generated-token"
  capabilities="urn:oracle:webcenter:read" />
```

Note: The security token is not used for authentication or identity propagation.

Security tokens are based on the authenticated user's name. They do not expire, making it possible to both cache and bookmark the URIs.

Security tokens are also "salted," a cryptographic technique of adding extra characters to a string before encrypting it. Because of salting, if a security token is compromised, you will not have to change the user's user name across the entire system to address the problem.

This technique prevents cases where a user name is compromised and you don't want to have to change the user name system wide to fix the problem.

For more information on security tokens, see "Security Considerations for WebCenter Portal REST APIs" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

27.4 Configuring a Proxy Server

This section explains how to set up a simple, response-rewriting reverse HTTP proxy on an Apache server. A proxy server is typically employed to avoid cross-domain request problems associated with making XMLHttpRequest (XHR) calls from a browser client. These calls are typically associated with the Ajax development technique for creating rich, interactive client-side interfaces. REST APIs are typically used within this kind of client-side development scenario.

Note: This section illustrates a simple example of setting up a proxy server on Apache. For more detailed information, refer to the Apache Server documentation available at <http://httpd.apache.org/docs>. You can also use Oracle HTTP Server (OHS) for your proxy server. For more information, see *Oracle Fusion Middleware Administrator's Guide for Oracle HTTP Server*.

The basic steps for setting up a proxy server on Apache are:

1. Obtain access to an Apache server. Oracle recommends Apache 2.2.7 or a later version.
2. Make sure the server has the `mod_substitute` module installed. Note that Apache versions 2.2.7 and later include `mod_substitute` by default. It is also possible to use `mod_sed` or `mod_line_edit`, however these configurations are not supported by Oracle.
3. Open the `httpd.conf` or the virtual host config file, and add the following lines, substituting your server name/information where appropriate:

```
ProxyRequests          Off
LoadModule             substitute_module      modules/mod_substitute.so
SetOutputFilter        SUBSTITUTE

ProxyPass              /rest/api/          http://myhost:8888/rest/api/
ProxyPassReverse       /rest/api/          http://myhost:8888/rest/api/
Substitute             s|myhost|yourhost|n

ProxyPass              /pathname/rest/api/    http://myhost:8888/rest/api/
ProxyPassReverse       /pathname/rest/api/    http://myhost:8888/rest/api/
Substitute             s|myhost:8888/rest/api|yourhost/pathname/rest/api|n
```

Note: Two servers are being proxied in this example scenario. Note that the following two calls are actually talking to these two different servers, but they appear to clients to be the same server host:

```
http://myhost/rest/api/resourceIndex
```

```
http://myhost/pathname/rest/api/resourceIndex
```

4. Restart the Apache server. For example, on Linux, you could do this:

```
sudo /etc/init.d/httpd restart
```

Note that on some configurations of Linux, proxying with Apache in this fashion requires you tell selinux to allow outbound connections from httpd. You can accomplish this by enabling the `httpd_can_network_connect` flag in selinux's GUI or through the command line.

Developer Tip: Set the `UserDir` permissions in `httpd.conf` to allow users to drop these files in their own `public_html` directory. For example, you might hit `http://host/~yourname/sample.html` to access your sample application, and then have the sample application make XHR calls to `http://host/rest/api/resourceIndex`.

27.5 Changing the REST Root Name

Although not required, in some cases you might want to change the root name for the REST APIs. The recommended technique for changing the REST root name is to do so by configuring a proxy server. For example, through the proxy server configuration described in [Section 27.4, "Configuring a Proxy Server,"](#) the following two URIs refer to the same server:

```
http://myhost:8888/rest/api/resourceIndex
```

```
http://myhost:8888/pathname/rest/api/resourceIndex
```

27.6 Using Compression

This section explains techniques for enabling compression on the XML or JSON responses that are returned to the client by the WebCenter Portal REST APIs.

If you are running Apache, you can add the `mod_deflate` or `mod_gzip` server modules to the server configuration. Refer to the Apache documentation for more information.

If you are using Oracle HTTP Server (OHS), Oracle recommends using Oracle Web Cache for this purpose. For detailed information, see *Oracle Fusion Middleware Administrator's Guide for Oracle Web Cache*.

If you are using OHS, you can also add the `mod_deflate` or `mod_gzip` server module to enable compression. For detailed information on this technique, see "Understanding Oracle HTTP Server Modules" in the *Oracle Fusion Middleware Administrators Guide for Oracle HTTP Server*.

For more information on Oracle Web Cache, see the section "Compression" in the *Oracle Fusion Middleware Administrators Guide for Oracle HTTP Server*, and see the chapter "Caching and Compressing Content" in the same guide.

27.7 Handling Authentication

By default, REST services are configured to accept authentication from identity assertion providers. If no identity assertion providers are configured, basic authentication is used.

For information on configuring identity assertion providers, see [Section 29.10, "Configuring the REST Service Identity Asserter."](#)

For more information, see "Configuring Authentication Providers" in *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

Note: Users can access the CMIS root anonymously. For more information, see "Security Considerations for CMIS REST APIs" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

Part V

Advanced Systems Administration for Oracle WebCenter Portal

Part V contains the following chapters:

- [Chapter 28, "Managing WebCenter Portal Application Security"](#)
- [Chapter 29, "Configuring the Identity Store"](#)
- [Chapter 30, "Configuring the Policy and Credential Store"](#)
- [Chapter 31, "Configuring Single Sign-on"](#)
- [Chapter 32, "Configuring Framework Applications for Single Sign-on"](#)
- [Chapter 33, "Configuring SSL"](#)
- [Chapter 34, "Configuring WS-Security"](#)
- [Chapter 35, "Configuring Security for Portlet Producers"](#)
- [Chapter 36, "Using WebCenter Portal Administration Console"](#)
- [Chapter 37, "Managing a Multilanguage Portal"](#)
- [Chapter 38, "Monitoring Oracle WebCenter Portal Performance"](#)
- [Chapter 39, "Managing Export, Import, Backup, and Recovery of WebCenter Portal"](#)

Managing WebCenter Portal Application Security

This chapter provides an introduction to securing WebCenter Portal: Framework applications, and describes the security configuration that is in place when Framework applications and Spaces applications are initially deployed. This chapter also includes a troubleshooting section that provides solutions for common security-related configuration issues.

This chapter includes the following sections:

- [Section 28.1, "Introduction to WebCenter Portal Application Security"](#)
- [Section 28.2, "Default Security Configuration"](#)
- [Section 28.3, "Troubleshooting Security Configuration Issues"](#)

For information about specific aspects of configuring security for WebCenter Portal applications (which include Framework and Spaces applications), see:

- [Chapter 29, "Configuring the Identity Store"](#)
- [Chapter 30, "Configuring the Policy and Credential Store"](#)
- [Chapter 31, "Configuring Single Sign-on"](#)
- [Chapter 32, "Configuring Framework Applications for Single Sign-on"](#)
- [Chapter 33, "Configuring SSL"](#)
- [Chapter 34, "Configuring WS-Security"](#)
- [Chapter 35, "Configuring Security for Portlet Producers"](#)
- [Chapter 36, "Using WebCenter Portal Administration Console"](#)

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."](#)

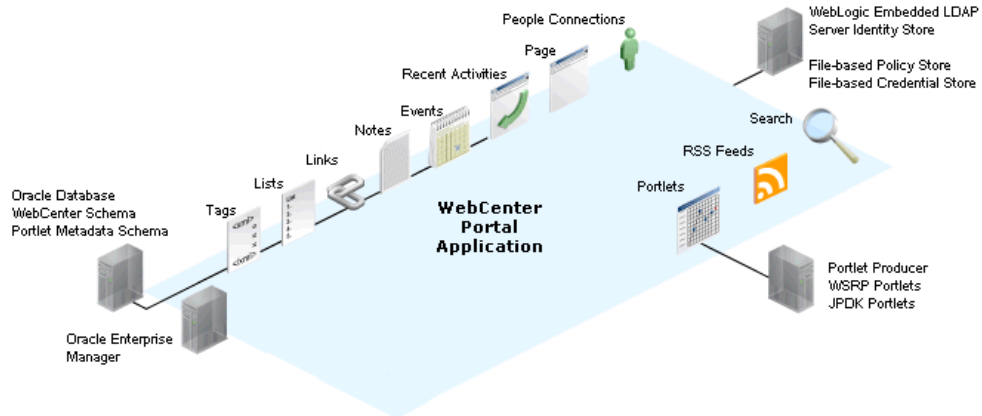
28.1 Introduction to WebCenter Portal Application Security

The recommended security model for WebCenter Portal applications 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.

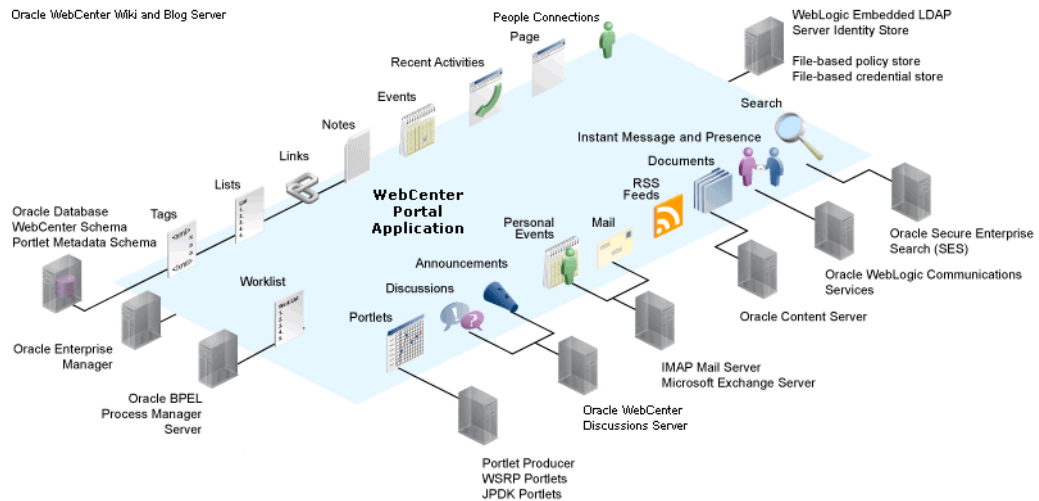
Figure 28–1 shows the relationship between a WebCenter Portal application deployment and its services, servers, portlets, portlet producers, its identity, credential and policy stores, and Oracle Enterprise Manager.

Figure 28–1 Basic WebCenter Portal Application Architecture

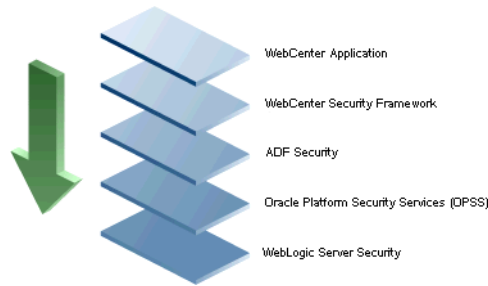


The diagram in Figure 28–2 shows a basic WebCenter Portal application after deployment with its back-end server connections.

Figure 28–2 WebCenter Portal Application Architecture with Back-end Server Connections



The diagram in Figure 28–3 shows the security layers for WebCenter Portal applications.

Figure 28–3 WebCenter Portal Security Layers

Framework applications and Spaces share the same four bottom security layers (WebCenter Security Framework, ADF Security, OPSS, and WebLogic Server Security). The application layer will, of course, depend on the implementation.

WebCenter Portal Application Security

WebCenter Portal provides support for:

- Application role management and privilege mapping
- Self-registration
- Space-level security management
- Account management
- External application credential management

WebCenter Portal Security Framework

WebCenter Portal Security Framework provides support for:

- Service Security Extension Framework (a common permission-based and role-mapping based model for specifying the security model for services)
- 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

28.2 Default Security Configuration

This section describes the security configuration that is in place when WebCenter Portal: Framework applications and WebCenter Portal: Spaces are deployed, and the tasks that must be carried out after deployment:

- [Section 28.2.1, "Administrator Accounts"](#)
- [Section 28.2.2, "Application Roles and Enterprise Roles"](#)
- [Section 28.2.3, "Default Identity and Policy Stores"](#)
- [Section 28.2.4, "Default Policy Store Permissions and Grants"](#)
- [Section 28.2.5, "Post-deployment Security Configuration Tasks"](#)

28.2.1 Administrator Accounts

Framework applications do not contribute any pre-seeded accounts, and therefore rely on the Fusion Middleware 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 the Spaces application does not contribute any pre-seeded accounts, there are certain pre-seeded grants that are given to the default Fusion Middleware administrator account (`weblogic`) for the Spaces application. If your installation does not use `weblogic` as the account name for the Fusion Middleware administrator role, you must configure one or more other users for this role as described in [Section 30.6, "Managing Users and Application Roles."](#)

Note: The `weblogic` account is a system administrator account and should not be used to create user-level artifacts. The `weblogic` account should only be used to create new user accounts in Fusion Middleware Control.

28.2.2 Application Roles and Enterprise Roles

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 an application-specific stripe of the 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 an application.

Within Spaces or a Framework application you can assign application roles and permissions to users in the corporate identity store. You can also assign application roles and permissions to enterprise roles defined in the enterprise identity store.

28.2.3 Default Identity and Policy Stores

By default, WebCenter Portal 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. For a list of supported identity store LDAP servers, see "Supported LDAP Identity Store Types" in the *Oracle Fusion Middleware Application Security Guide*.

The default file-based policy store should only be used for development, and only for single-node Spaces configurations. For enterprise deployments you must reassociate the policy and credential store with a database, or with an external LDAP-based store as described in [Chapter 30, "Configuring the Policy and Credential Store."](#)

The policy and credential stores can use either Oracle Internet Directory 11gR1 or 10.1.4.3, or Oracle RDBMS (releases 10.2.0.4 or later; releases 11.1.0.7 or later; and releases 11.2.0.1 or later). Note that when using an external LDAP-based store, the policy and credential stores must use the same LDAP server. Similarly, when using a database, the policy and credential stores must use the same database.

For more information about the supported identity store and policy and credential store configurations, see "Supported LDAP-, DB-, and File-Based Services" in the *Oracle Fusion Middleware Application Security Guide*. For more information on reconfiguring the identity, policy and credential stores, see [Chapter 29, "Configuring the Identity Store"](#) and [Chapter 30, "Configuring the Policy and Credential Store."](#)

Note: By default, WebCenter Portal's Discussions service is configured to use the embedded LDAP identity store: All users in the embedded LDAP store can log on to the discussions server, and all users in the Administrators group have administrative privileges on the discussions server.

If you reassociate the identity store with an external LDAP server, you must either move the Fusion Middleware administrator account to the external LDAP (as described in [Section 29.5, "Moving the Administrator Account to an External LDAP Server"](#)), or if you choose not to move the administrator account, you must perform some additional steps to identify the new administrator account for the discussions server as described in [Section 29.5.1, "Migrating WebCenter Portal's Discussions Server to Use an External LDAP."](#)

For Spaces, both Spaces and Content Server must share the same LDAP server. For more information, see [Section 29.6, "Configuring the Oracle Content Server to Share the Spaces Identity Store LDAP Server."](#)

28.2.3.1 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.

28.2.4 Default Policy Store Permissions and Grants

The ADF Security permissions model supports both permission-based and role-based authorization. These two types of authorization, and the default Policy Store permissions and code based grants are discussed in the following sections:

- [Section 28.2.4.1, "Permission-based Authorization"](#)
- [Section 28.2.4.2, "Role-mapping Based Authorization"](#)
- [Section 28.2.4.3, "Default Policy Store Permissions for Spaces"](#)
- [Section 28.2.4.4, "Default Code-based Grants"](#)

28.2.4.1 Permission-based Authorization

Permission-based authorization is used for services, such as Lists, where access control is implemented within the WebCenter Portal application using Oracle Platform Security Services (OPSS). 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 Spaces, see "Managing Application Roles and Permissions" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

28.2.4.2 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 users of a WebCenter Portal application (mapping to one or more application roles) must be mapped to another set of roles on the discussions server.

For example, in the Spaces application:

- Spaces roles are mapped to corresponding roles on the back-end discussions server.
- When a user is granted a new Spaces space role, a similar grant (privilege) is granted in the back-end discussions server. For example, when user Pat is granted `Discussions-Create/Edit/Delete` permissions in Spaces, Pat is granted corresponding permissions in the back-end discussions server.

See also, "Understanding Discussions Server Role and Permission Mapping" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

28.2.4.3 Default Policy Store Permissions for Spaces

Out-of-the box, Spaces provides the following default roles:

Default application roles:

- Administrator
- Authenticated-User
- Public-User

For more information about the default application roles, see "Default Permissions for Application Roles" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

Default roles in a space:

- Moderator
- Participant
- Viewer

For more information about the default role within a space, see "Default Permissions for Roles in a Space" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

28.2.4.4 Default Code-based Grants

WebCenter Portal applications make internal calls to APIs on the security platform that are secured with permission checks. Consequently, the WebCenter Portal application must be granted appropriate permissions to invoke the OPSS APIs (for example, the permission to access the policy store and grant or revoke permissions (`PolicyStoreAccessPermission`), or grant basic permissions to application roles). In the case of Spaces, basic application role permissions are granted by default as described in "Default Permissions for Application Roles" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

Similarly, WebCenter Portal applications must pre-authorize access to various operations that it wants to expose using the WebCenter Portal permissions, and then invoke the OPSS APIs as privileged actions.

28.2.5 Post-deployment Security Configuration Tasks

After deploying your Framework application or Spaces, consider the following security-related configuration tasks for your site:

- **Reassociating the identity store to use an external LDAP**

By default, WebCenter Portal applications use an embedded LDAP for their 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 [Chapter 29, "Configuring the Identity Store."](#)

Note: By default, Oracle WebCenter Portal's Discussions Server is configured to use the embedded LDAP identity store. All users in the embedded LDAP store can log on to the discussions server, and all users in the `Administrators` group have administrative privileges on the discussions server.

If you reassociate the identity store with an external LDAP server, you must either move the Fusion Middleware administrator account to the external LDAP (as described in [Section 29.5, "Moving the Administrator Account to an External LDAP Server"](#)), or if you choose not to move the administrator account, you must perform some additional steps to identify the new administrator account for the discussions server as described in [Section 29.5.1, "Migrating WebCenter Portal's Discussions Server to Use an External LDAP."](#)

For Spaces, both Spaces and Content Server must share the same LDAP server. For more information, see [Section 29.6, "Configuring the Oracle Content Server to Share the Spaces Identity Store LDAP Server."](#)

- **Reassociating the policy store to use an external LDAP or database**

By default, Framework applications use a file-based `system-jazn-data.xml` policy store to store policy grants. You should consider using an LDAP-based or database policy store. For information on how to configure the policy store to use an LDAP server or database, see [Chapter 30, "Configuring the Policy and Credential Store."](#)

- **Configuring WS-Security**

Although the use of WS-Security adds complexity to the configuration and management of a Framework application and the set of producers it consumes, it helps ensure the security of the information being published by the Framework application. Adding WS-Security provides authentication for the consumer, and message-level security.

For information on how to configure WS-Security for Framework applications and components, see [Chapter 34, "Configuring WS-Security."](#)

- **Configuring SSO**

Single Sign-On (SSO) allows users to log in once across WebCenter Portal applications and components rather than having to log in for each sub-application (for example, for accessing a wiki page in 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 Portal 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 Portal 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 [Chapter 31, "Configuring Single Sign-on."](#)

- **Configuring SSL**

Secure Sockets Layer (SSL) provides additional security for connections between WebCenter Portal applications or components by providing an additional

authentication layer, and by encrypting the data exchanged. For connections between applications or components where the data exchanged 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 [Chapter 33, "Configuring 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.

28.3 Troubleshooting Security Configuration Issues

This section includes the following sub-sections:

- [Section 28.3.1, "Spaces Application Does Not Find Users in LDAP Provider"](#)
- [Section 28.3.2, "Space Created with Errors When Logged in as OID User"](#)
- [Section 28.3.3, "Users Cannot Self-Register when Spaces Configured with Active Directory"](#)
- [Section 28.3.4, "User Made Administrator Does Not Have Administrator Privileges"](#)
- [Section 28.3.5, "OmniPortlet Producer Authorization Exception in SSO Environment"](#)
- [Section 28.3.6, "Deploying the SAML SSO-specific Discussions EAR file Produces an Exception"](#)
- [Section 28.3.7, "Configuring SAML Single Sign-on Produces 403 Error"](#)

28.3.1 Spaces Application Does Not Find Users in LDAP Provider

Problem

Weblogic Server was configured with an external LDAP provider. Users in the external LDAP can log in to Spaces, but when you try to assign the administrator role, in Spaces, to a user from the external LDAP, no users are found.

Solution

Change the Control Flag for the `DefaultAuthenticator` Authentication Provider to `Sufficient` as described in [Chapter 29, "Configuring the Identity Store."](#) Restart the Administration Server and Managed Servers for the domain.

28.3.2 Space Created with Errors When Logged in as OID User

Problem

When logged in to Spaces as an OID user (for example, `orcladmin`), and you try to create a space, the space gets created but with errors. The error message appears as "No matching users were found with search string <login user>".

Solution

The following property is missing in the `jps-config.xml` file:

```
<property name="jps.user.principal.class.name"
value="weblogic.security.principal.WLSUserImpl" />
```


To fix this:

1. Edit `DOMAIN_HOME/config/fmwconfig/jps-config.xml`.
2. Add this line in the general properties:


```
<property name="jps.user.principal.class.name"
value="weblogic.security.principal.WLSUserImpl"/>
```
3. Restart the `WC_Spaces` server.

28.3.3 Users Cannot Self-Register when Spaces Configured with Active Directory

Problem

Users cannot self-register with Active Directory after configuring Spaces to use AD authenticator. When a user tries to self-register, the following error message appears:

"User not created. Either the user name or the password does not adhere to the registration policy or the identity store is unavailable. Specify the required user credentials or contact your administrator for assistance."

Solution

To fix the problem:

1. Set the user name attribute to `sAMAccountName` while configuring Active Directory in the WebLogic Administration Console.
2. Use the HTTPS port of the LDAP and enable the SSL checkbox while configuring Active Directory in the WebLogic Administration Console.

28.3.4 User Made Administrator Does Not Have Administrator Privileges

Problem

After logging in as `orcladmin` and making a user an administrator, after logging out and logging in as that user, the Administrator link is still not available.

Solution

The problem is due to duplicate `cn` entries in the identity store. Since `cn` is mapped to the username attribute, it must be unique. Remove the duplicate from the identity store and the user should have the appropriate `privileges.cn`.

28.3.5 OmniPortlet Producer Authorization Exception in SSO Environment

Problem

OmniPortlet producer receives an authorization exception when it tries to store connection information in the Credential Store Framework (CSF) wallet when WebCenter Portal is configured with SSO.

Solution

Grant the required permissions to `ssofilter.jar` by connecting to the Oracle WebCenter Portal Administration Server using WLST (for more information, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands"](#)) and running the following grant commands:


```

grantPermission(codeBaseURL="file:${oracle.home}/modules/oracle.ssofilter_11.1.1/s
sofilter.jar",
permClass="oracle.security.jps.service.credstore.CredentialAccessPermission",
permTarget="context=SYSTEM,mapName=omniportlet_user,keyName=*",
permActions="*")

grantPermission(codeBaseURL="file:${oracle.home}/modules/oracle.ssofilter_11.1.1/s
sofilter.jar",
permClass="oracle.security.jps.service.credstore.CredentialAccessPermission",
permTarget="context=SYSTEM,mapName=omniportlet_default,keyName=*",
permActions="*")
grantPermission(codeBaseURL="file:${oracle.home}/modules/oracle.ssofilter_11.1
.1/ssofilter.jar",
permClass="oracle.security.jps.service.credstore.CredentialAccessPermission",
permTarget="context=SYSTEM,mapName=omniportlet_user,keyName=*",
permActions="*")
    
```

28.3.6 Deploying the SAML SSO-specific Discussions EAR file Produces an Exception

Problem

Undeploying the Discussions EAR file and deploying the SAML SSO-specific Discussions EAR file and then starting the application in the WLS Administration Console produces the following exception:

```

java.lang.ClassCastException:
org.apache.xerces.parsers.XIncludeAwareParserConfiguration
    
```

Solution

Restart the `WC_Collaboration` server. This should fix the issue and the Discussions application will be in an active state.

28.3.7 Configuring SAML Single Sign-on Produces 403 Error

Problem

While testing a SAML SSO configuration you encounter 403 errors, and after turning on debug logging, as described in [Section 31.4.2.4, "Checking Your Configuration,"](#) you see the following kind of error logs in the destination server:

```

####<Oct 11, 2010 10:20:31 PM PDT> <Debug> <SecuritySAMLlib> <adc2170966>
<soa_server1> <[ACTIVE] ExecuteThread: '1' for queue:
'weblogic.kernel.Default (self-tuning) '> <<WLS Kernel>> <>
<efaf471a17d5a745:-5ba0524a:12b9b0b7849:-8000-0000000000015385>
<1286860831335> <BEA-000000> <SAMLSignedObject.verify(): validating
signature>
####<Oct 11, 2010 10:20:31 PM PDT> <Debug> <SecuritySAMLService> <adc2170966>
<soa_server1> <[ACTIVE] ExecuteThread: '1' for queue:
'weblogic.kernel.Default (self-tuning) '> <<WLS Kernel>> <>
<efaf471a17d5a745:-5ba0524a:12b9b0b7849:-8000-0000000000015385>
<1286860831336> <BEA-000000> <SAMLDestinationSiteHelper: Signature
verification failed with exception: org.opensaml.InvalidCryptoException:
SAMLSignedObject.verify() failed to validate signature value>
####<Oct 11, 2010 10:20:31 PM PDT> <Debug> <SecuritySAMLService> <adc2170966>
<soa_server1> <[ACTIVE] ExecuteThread: '1' for queue:
'weblogic.kernel.Default (self-tuning) '> <<WLS Kernel>> <>
<efaf471a17d5a745:-5ba0524a:12b9b0b7849:-8000-0000000000015385>
<1286860831336> <BEA-000000> <SAMLDestinationSiteHelper: Unable to validate
    
```

```
response -- returning SC_FORBIDDEN>
###<Oct 11, 2010 10:20:31 PM PDT> <Debug> <SecuritySAMLService> <adc2170966>
<soa_server1> <[ACTIVE] ExecuteThread: '1' for queue:
'weblogic.kernel.Default (self-tuning) ' > <<WLS Kernel>> <>
<efaf471a17d5a745:-5ba0524a:12b9b0b7849:-8000-0000000000015385>
<1286860831336> <BEA-000000> <SAMLSingleSignOnService.doACSGet: Failed to get
SAML credentials -- returning>
```

Solution

Chances are that something went wrong with your certificate setup due to which SAML assertions are not getting validated. This is likely because the certificate registered in the SAML Identity asserter is incorrect. Export the certificate used for SAML SSO setup in the Spaces domain specified by `certAlias` and `certPassword` and copy it to a accessible location in the destination domain.

1. Update the relevant config section in the `wcsamlssso.properties` file in the Spaces domain (for example, if the certificate was invalid for the SOA configuration, update the `certPath` in the `soa_config` section).
2. Open the WebLogic Server Admin Console, and from the `WC_Spaces` domain go to **Security Realm > Providers > Credential Mapping > wcsamlcm > Management > Relying Parties** and delete the relying parties relevant to the domain (for example, for SOA, they would be Worklist Integration, Worklist Detail, and Worklist SDP.)
3. Go to **Destination Domain > Security Realm > Providers > Authentication > wcsamlia > Management > Asserting Parties** and delete the corresponding asserting parties.
4. Open the Certificates tab and delete the certificate as well.
5. Go back to the Spaces domain and re-run the scripts for creating asserting-relying parties pairs. For SOA, for example, you would need to re-run:

```
$WC_ORACLE_HOME/webcenter/scripts/samlssso/configureWorklistIntegration.py
$WC_ORACLE_HOME/webcenter/scripts/samlssso/configureWorklistDetail.py
$WC_ORACLE_HOME/webcenter/scripts/samlssso/configureWorklistSDP.py
```

6. Test your configuration again. If all works well, you can disable SAML logging.

Configuring the Identity Store

This chapter describes how to reassociate the identity store with an external LDAP rather than the default embedded LDAP identity store. It also describes how to configure an LDAP server for Oracle WebCenter Content Server and contains the following subsections:

- [Section 29.1, "Reassociating the Identity Store with an External LDAP Server"](#)
- [Section 29.2, "Tuning the Identity Store for Performance"](#)
- [Section 29.3, "Configuring the GUID Attribute for External LDAP Identity Stores"](#)
- [Section 29.4, "Adding Users to the Embedded LDAP Identity Store"](#)
- [Section 29.5, "Moving the Administrator Account to an External LDAP Server"](#)
- [Section 29.6, "Configuring the Oracle Content Server to Share the Spaces Identity Store LDAP Server"](#)
- [Section 29.7, "Aggregating Multiple Identity Store LDAP Servers Using libOVD"](#)
- [Section 29.8, "Configuring Dynamic Roles for the Spaces Application"](#)
- [Section 29.9, "Configuring Dynamic Groups for the Spaces Application"](#)
- [Section 29.10, "Configuring the REST Service Identity Asserter"](#)

Caution: Before reassociating the identity store, be sure to back up the relevant configuration files:

- `config.xml`
- `jps-config.xml`

As a precaution, you should also back up the `boot.properties` file for the Administration Server for the domain.

Note that for Framework applications, the steps for [Migrating WebCenter Portal's Discussions Server to Use an External LDAP](#) are not required. For more information about the identity store, see the *Oracle Fusion Middleware Application Security Guide*.

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."](#)

29.1 Reassociating the Identity Store with an External LDAP Server

In almost all cases, you must reassociate the identity store with an external LDAP server rather than using the default embedded LDAP. Although you can use many different types of LDAP servers (see [Section 28.2, "Default Security Configuration"](#) for a list of supported LDAPs), this section focuses on how to configure the identity store to use Oracle Internet Directory (OID). For configuration settings for other supported LDAP servers, see "Mapping User Attributes to LDAP Directories" in the *Oracle Fusion Middleware Application Security Guide* for the user attribute mappings specific to those LDAPs.

Caution: Reassociating an external LDAP identity store (such as OID) in a production environment with another external LDAP store is not supported. If you have a business need to carry out such a reassociation, please contact Oracle support before going ahead as user information and artifacts may be lost in the process.

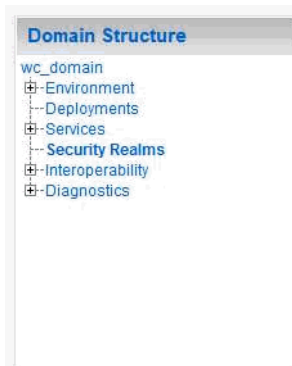
To reassociate the identity store with OID:

1. Log in to the WebLogic Server Administration Console.

For information on logging into the WebLogic Server Administration Console, see [Section 1.13.2, "Oracle WebLogic Server Administration Console."](#)

2. In the Domain Structure pane (see [Figure 29–1](#)), click **Security Realms**.

Figure 29–1 Domain Structure Pane



The Summary of Security Realms pane displays (see [Figure 29–10](#)).

Figure 29–2 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

- In the Name column, click the realm for which you want to reassociate the identity store.

The Realm Settings pane displays (see [Figure 29–3](#)).

Figure 29–3 Realm Settings Pane

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...](#)

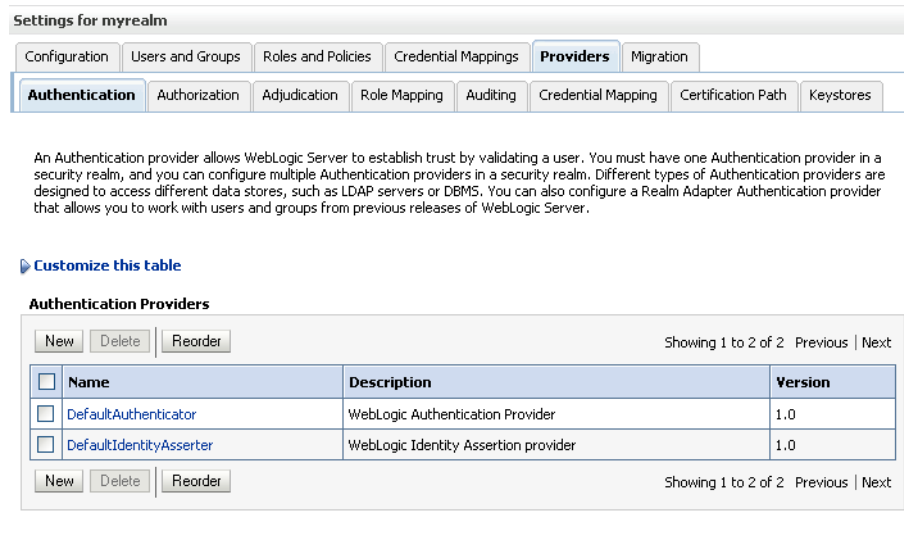
Advanced

Save

4. Open the **Providers** tab.

The Providers Settings pane displays (see [Figure 29–4](#)).

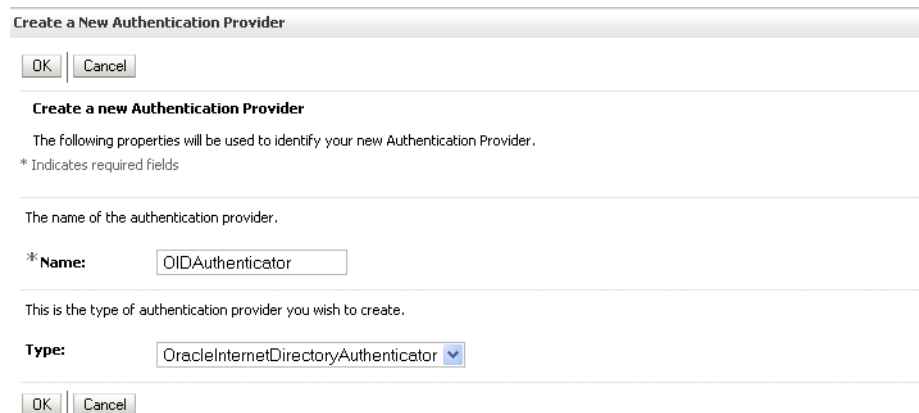
Figure 29–4 Settings Pane - Providers



5. Click **New** to add a new provider.

The Create a New Authentication Provider pane displays (see [Figure 29–5](#)).

Figure 29–5 Create a New Authentication Provider Pane



6. Enter a name for the provider (for example `OIDAuthenticator` for a provider that authenticates 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`.

8. Click **OK** to save your settings.

The Settings pane displays with the new authentication provider (see [Figure 29–6](#)).

Figure 29–6 Settings Pane - Authentication 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 3 of 3 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
<input type="checkbox"/>	OIDAuthenticator	Provider that performs LDAP authentication	1.0

New Delete Reorder Showing 1 to 3 of 3 Previous | Next

- In the list of Authentication Providers, click the newly created provider.

The Settings Pane for the new authentication provider displays (see [Figure 29–7](#)).

Figure 29–7 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: OIDAAuthenticator The name of this Oracle Internet Directory Authentication provider. [More Info...](#)

Description: Provider that performs LDAP authentication A short description of this Oracle Internet Directory Authentication provider. [More Info...](#)

Version: 1.0 The version number of this Oracle Internet Directory Authentication provider. [More Info...](#)

Control Flag: SUFFICIENT Specifies how this Oracle Internet Directory Authentication provider fits into the login sequence. [More Info...](#)

Save

- 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 falls 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 29–8](#)).

Figure 29–8 Provider Specific Pane

Settings for OIAuthenticator

Configuration Performance

Common Provider Specific

Save

Use this page to define the provider specific configuration for this Oracle Internet Directory Authentication provider.

Connection

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:

SSLEnabled Specifies whether the SSL protocol should be used when connecting to the LDAP server. [More Info...](#)

Users

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...](#)

13. Enter the details specific to *your* LDAP server.

Note: The table below shows values appropriate for OID. For the permissible values for other LDAPs, such as Active Directory, see the appendix "OPSS System and Configuration Properties" in the *Oracle Fusion Middleware Application Security Guide*.

Parameter	Value	Description
Host:		The LDAP server's server ID (for example, <ldap_host>example.com)

Parameter	Value	Description
Port:		The LDAP server's port number (for example, 3060)
Principal:		The LDAP user DN used to connect to the LDAP server (for example, cn=orcladmin)
Credential:		The password used to connect to the LDAP server
User Base DN:		Specify the DN under which your Users start (for example, cn=users, dc=example, dc=com)
Group Base DN:		Specify the DN that points to your Groups node (for example, cn=groups, dc=example, dc=com)
Use Retrieved User Name as Principal	Checked	Must be turned on
All Users Filter:	(&(uid=*)(objectclass=person))	Search to find all users under the User Base DN
User From Name Filter:	(&(uid=%u)(objectclass=person))	
User Name Attribute:	uid	

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 29.5, "Moving the Administrator Account to an External LDAP Server."](#)

Note: Do not use the `REQUIRED` control flag if you are using multiple authenticators. If a `REQUIRED` control flag is found in the list of authenticators, regardless of its position, no further authenticators will be examined.

- 16. Restart the Administration Server and the managed server for the changes to take effect.**

29.2 Tuning the Identity Store for Performance

The following sections describe performance-related configurations that may be required for specific environments. For more general information about tuning and

performance for WebCenter Portal, see *Oracle Fusion Middleware Performance and Tuning Guide*.

This section includes the following subsections:

- [Section 29.2.1, "Tuning the Identity Store when Using SSL"](#)
- [Section 29.2.2, "Tuning Performance when Using OVD"](#)
- [Section 29.2.3, "Tuning Performance when Using Active Directory"](#)

29.2.1 Tuning the Identity Store when Using SSL

When you configure an identity store with WebCenter Portal (using WebLogic Server providers), you can choose to configure either an SSL port or a non-SSL port. If you choose an SSL port, by default, the JNDI connections are not pooled causing increased response time and decreased performance when looking up users, groups, or other identity store entities. To address this, do the following:

1. Open the `jps-config.xml` file under `domain_home/config/fmwconfig/jps-config.xml`, locate the `idstore.ldap` service instance and add the line highlighted below:

```
<!-- 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="CONNECTION_POOL_CLASS"
value="oracle.security.idm.providers.stddap.JNDIPool" />
    <property name="java.naming.ldap.factory.socket"
value="javax.net.ssl.SSLSocketFactory" />
  </serviceInstance>
```

2. Restart all the servers within the domain that are connected to the identity store on an SSL port with the following JVM parameter:

```
-Dcom.sun.jndi.ldap.connect.pool.protocol=ssl
```

You can specify this by modifying `setDomainEnv.sh` or directly from the console.

3. Verify that the servers are running with this JVM parameter, and then (for *nix systems) run the following `grep` command:

```
ps -aef | grep WC_Spaces
```

and verify that the process state specifies

```
com.sun.jndi.ldap.connect.pool.protocol=ssl.
```

29.2.2 Tuning Performance when Using OVD

For OVD, the only object class against which attributes are looked up is `inetOrgPerson` (and its parent object classes). Since the Profile Gallery can display attributes not defined in `inetOrgPerson`, all the additional attributes not covered in `inetOrgPerson` would require an additional round trip to the identity store.

For best performance when using OVD in a production environment, Oracle recommends that you add the following configuration entry (in bold) to the domain-level `jps-config.xml` file:

```
<!-- 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="CONNECTION_POOL_CLASS"
value="oracle.security.idm.providers.stddldap.JNDIPool"/>

      <extendedProperty>
        <name>user.object.classes</name>
        <values>
          <value>top</value>
          <value>person</value>
          <value>inetorgperson</value>
          <value>organizationalperson</value>
          <value>orcluser</value>
          <value>orcluserv2</value>
          <value>ctCalUser</value>
        </values>
      </extendedProperty>
    </serviceInstance>

```

29.2.3 Tuning Performance when Using Active Directory

For best performance when using Active Directory in a production environment, Oracle recommends that you add the following configuration entries (in bold) to the domain-level `jps-config.xml` file:

```

    <serviceInstance provider="idstore.ldap.provider"
name="idstore.ldap">
      <property
value="oracle.security.jps.wls.internal.idstore.WlsLdapIdStoreConfigProvider"
name="idstore.config.provider"/>
      <property value="oracle.security.idm.providers.stddldap.JNDIPool"
name="CONNECTION_POOL_CLASS"/>
      <property name="PROPERTY_ATTRIBUTE_MAPPING"
value="WIRELESS_ACCT_NUMBER=mobile:MIDDLE_NAME=middlename:MAIDEN_NAME=sn:DATE_OF_HIRE=pwdLastSet:NAME_SUFFIX=generationqualifier:DATE_OF_BIRTH=pwdLastSet:DEFAULT_GROUP=primaryGroupID" />
      <property value="sAMAccountName" name="username.attr"/>
      <property value="sAMAccountName" name="user.login.attr"/>
    </serviceInstance>

```

The People Profile Service queries for all these attributes and there is no default mapping for these attributes in the Active Directory provider. A vanilla Active Directory installation doesn't have any mapping corresponding to `DATE_OF_HIRE`, `DATE_OF_BIRTH`.

Note that the two attributes are simply a mapping to some attribute of the correct data type to reduce unnecessary LDAP server calls as Active Directory really doesn't have corresponding attributes with the same semantic meaning.

29.3 Configuring the GUID Attribute for External LDAP Identity Stores

This section describes the different GUID attributes used by non-Oracle LDAP implementations, as shown below:

IBM Tivoli® Directory Server:

```
ibm-entryUUID
```

Microsoft® Active Directory:

objectGUID

If you are using Active Directory, remember that the `samAccountName` attribute has a 20-character limit; other IDs used by Lotus Connections have a 256-character limit.

Microsoft Active Directory Application Mode (ADAM):

objectGUID

To use `objectSID` as the default for ADAM, add the following line to the `<config:attributeConfiguration>` section of the `wimconfig.xml` file:

```
<config:externalIdAttributes name="objectSID" syntax="octetString"/>
```

BM Domino® Enterprise Server:

dominoUNID

Note that if the bind ID for the Domino LDAP does not have sufficient manager access to the Domino directory the Virtual Member Manager (VMM) does not return the correct attribute type for the Domino schema query; DN is returned as the VMM ID.

To override VMM's default ID setting, add the following line to the `<config:attributeConfiguration>` section of the `wimconfig.xml` file:

```
<config:externalIdAttributes name="dominoUNID"/>
```

Sun Java™ System Directory Server:

nsuniqueid

eNovell Directory Server:

GUID

If you are using an LDAP identity store that does not use the `orclGuid` attribute, such as IBM Tivoli, you must manually map the `GUID` attribute so that it matches your identity store. For example, for IBM Tivoli, set `GUID=ibm-entryUUID` in the `jps-config.xml` file as shown below:

1. Open the `MW_HOME/user_projects/domains/my_domain/config/fmwconfig/jps-config.xml` file in a text editor.

2. Set the `GUID` property as follows:

```
<serviceInstance provider="idstore.ldap.provider" name="idstore.ldap.0">
  <!-- existing props ... -->
  <property name="PROPERTY_ATTRIBUTE_MAPPING"
value="GUID=ibm-entryUUID"/>
  <extendedProperty>
    ... ..
  </extendedProperty>
</serviceInstance>
```

3. Restart all the servers.

29.4 Adding Users to the Embedded LDAP Identity Store

You can add users to the embedded LDAP using the WebLogic Server Administration Console, or using an LDIF file and LDAP commands. Using an LDIF file lets you add additional attributes not available through the WebLogic Server Administration Console.

Note: The embedded LDAP server should only be used for testing or "proof of concept." For production use, Oracle recommends using external identity stores, such as Oracle Internet Directory or Microsoft Active Directory, that are supported by the OPSS user and role APIs.

For Oracle Internet Directory, 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*).

Note: If you are planning to reassociate your identity store with an external LDAP, perform that step first (as described in [Section 29.1, "Reassociating the Identity Store with an External LDAP Server"](#)) as when you reassociate the embedded LDAP with OID or other external LDAP implementation users and user artifacts may not be carried forward. Consequently, do not add users to the embedded LDAP with the expectation of moving them to a production environment. The embedded LDAP is intended to be used only as a test environment, and is not intended as a staging environment that can be moved to production.

Spaces supports self-registration. New users who self-register with Spaces are added directly to the identity store. For more information about self-registration, see "Allowing Self-Registration" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

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:

- [Section 29.4.1, "Adding Users to the Identity Store Using the WLS Administration Console"](#)
- [Section 29.4.2, "Adding Users to the Identity Store Using an LDIF File"](#)

29.4.1 Adding Users to the Identity Store Using the WLS Administration Console

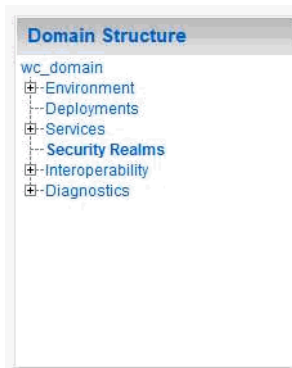
To add users to the embedded LDAP identity store from the WebLogic Server Administration Console:

1. Log in to the WebLogic Server Administration Console.

For information on logging into the WebLogic Server Administration Console, see [Section 1.13.2, "Oracle WebLogic Server Administration Console."](#)

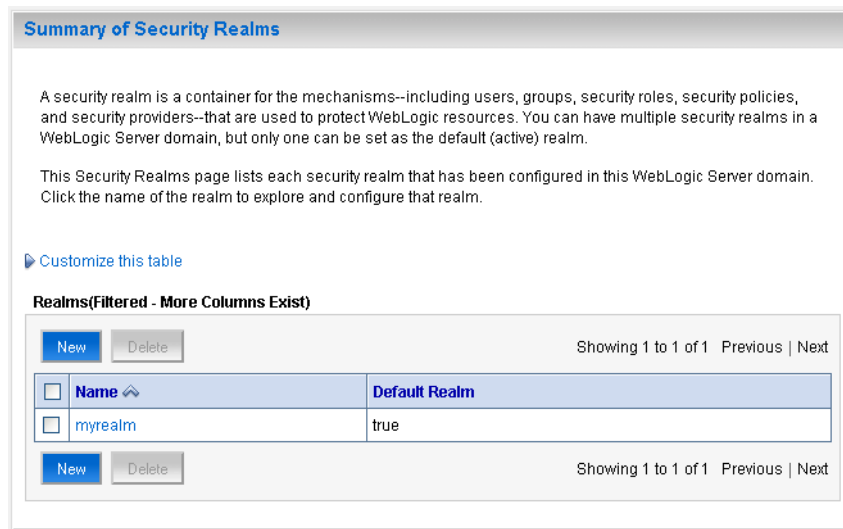
2. In the Domain Structure pane (see [Figure 29-9](#)), click **Security Realms**.

Figure 29–9 Domain Structure Pane



The Summary of Security Realms pane displays (see [Figure 29–10](#)).

Figure 29–10 Summary of Security Realms pane



3. In the Name column, click the realm to which you want to add users.
The Realm Settings pane displays (see [Figure 29–11](#)).

Figure 29–11 Realm Settings Pane

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...
<input checked="" type="checkbox"/> 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...
<input type="checkbox"/> 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. Click the **Users and Groups** tab to display the list of current users.
5. Click **New** to add a new user.

Figure 29–12 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

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 `DefaultAuthenticator`.
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. Reenter 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.

29.4.2 Adding Users to the Identity Store Using an LDIF File

You can add users directly to the embedded LDAP identity store using an LDIF file. Using an LDIF file enables you to specify additional user attributes that are not available through the WebLogic Server Administration Console.

As the embedded LDAP server is a conformant LDAP server, you can use LDAP commands to add or modify users. You can also search the directory, which is useful when exporting and importing user accounts.

To add users to the embedded LDAP using an LDIF file you must perform the following tasks:

- [Enable External LDAP Access](#)
- [Create an LDIF File](#)
- [Add the Users](#)

Enable External LDAP Access

When WebLogic Server 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 must reset the access credential for the embedded LDAP.

To reset the access credential for the embedded LDAP:

1. Log in to the WebLogic Server Administration Console.

For information on logging into the WebLogic Server Administration Console, see [Section 1.13.2, "Oracle WebLogic Server Administration Console."](#)

2. In the Domain Structure pane (see [Figure 29–13](#)), click `wc_domain`.

Figure 29–13 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 29–14](#)).

Figure 29–14 Settings Pane with Embedded LDAP Settings

4. Enter a new password in the **Credential** field, and reenter 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:

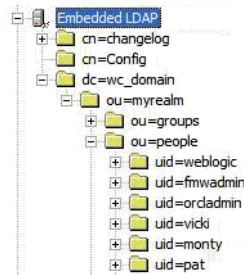
- the DN value for admin access is "cn=Admin"
- the password is the value you entered in the Credential field
- the port is the same as the admin port, which by default is 7001

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 WebLogic Server 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 29–15](#).

Figure 29–15 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 Spaces user profile screens:

```
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: Spaces user profiles include some attributes that are only available in Oracle Internet Directory. These include the following attributes from the `orclUserV2` objectclass:

- `orclTimeZone`
- `orclDateOfBirth`
- `maidenName`

You cannot add these attributes to an embedded LDAP identity store.

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 Identity Management User Reference*.

```
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 employeenumber:
    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

```

29.5 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 Fusion Middleware administrator account (`weblogic` by default) to the LDAP server.

If the Fusion Middleware 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, including the administrator account, are authenticated against 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 WebLogic Server to start and stop servers and do other administrator operations from the WebLogic Server Administration Console. If you keep the `DefaultAuthenticator`, make sure that the control flag for the `DefaultAuthentication` provider is set to `SUFFICIENT`. If you choose this option, you must also perform the additional steps described in [Section 29.5.1, "Migrating WebCenter Portal's Discussions Server to Use an External LDAP."](#)

Note: If the `weblogic` user account is used from the `DefaultAuthenticator`, this account should not be used to access the Spaces application as the application code will not be able to find the user in the external LDAP store.

- 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 or other named group that contains the list of users that are allowed to manage your domain in OID or other external LDAP. If a name other than "Administrators" is used, then you must update the group name in the definition of the WebLogic Server Global Administrator role. By default, this is defined as membership in the enterprise group called "Administrators". For information about changing the administrator group name, see [Section 29.5.2, "Changing the Administrator Group Name."](#)

29.5.1 Migrating WebCenter Portal's Discussions Server to Use an External LDAP

If you've installed Oracle WebCenter Portal's Discussions Server and choose **not to move** the administrator account to an external LDAP (as described in [Section 29.5, "Moving the Administrator Account to an External LDAP Server"](#)), you must perform some additional steps to identify the new administrator account for the discussions server prior to reordering the authenticators on the WebLogic Server:

1. Select a user account from the external LDAP to be the administrator for the discussions server.
2. Create an administrator account in the `DefaultAuthenticator` (that is, the embedded LDAP) that matches the one you selected from the external LDAP. The account names in the embedded LDAP and the external LDAP server must be the same.

For information about adding users to the embedded LDAP, see [Section 29.4, "Adding Users to the Embedded LDAP Identity Store."](#)

3. Log in to the Oracle WebCenter Portal's Discussion Server Admin Console with the boot-identity account (that is, `weblogic`) at:

```
http://host:port/owc_discussions/admin
```

Where *host* and *port* are the host ID and port number of the `WLS_Services` managed server.

4. Click **Settings > Admins/Moderators**.

The Admins & Moderators page displays (see [Figure 29-16](#)).

Figure 29–16 Admins & Moderators Page

Admins & Moderators Main » Admins & Moderators

Global category admin or system admin privileges to users or groups. Note, this sets permission for admins over all categories. To designate administrators for individual categories or forums, click on the "Content" tab, choose a category or forum then choose "Admins/Moderators" from the left menu.

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						
		System Admin	Category Admin	User Admin	Group Admin	Moderator	Remove
Users							
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Groups							
	administrators	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Save Changes Cancel

Legend

- * - Special permission type - Anyone and Registered Users cannot be removed, only cleared.
- System admin - do not delete all system admin users. You need at least one to log in to this tool.
- Permission is inherited because it has already been set globally or for a parent forum/category.
- Permission has been explicitly blocked in a parent forum/category.
- Indicates a permission is set.

5. Click Grant New Permissions.

The Grant New Permissions pane displays (see [Figure 29–17](#)).

Figure 29–17 Grant New Permissions Pane

Grant New Permissions

Permission Summary Grant New Permissions

Follow the steps below to grant new user or group permissions: Note, it is not possible to set permissions for "Anyone" or "Registered Users" here. To do this, use the Permissions Summary page.

- Choose the permissions: [\[select all\]](#)
 - System Admin
 - Category Admin
 - User Admin
 - Group Admin
 - Moderator
- Choose a user or group to grant the permissions to:
 - A Specific User: (enter username - separate multiple usernames with commas)
 - A Specific Group: (enter group name - separate multiple group names with commas)
- Done:

Grant New Permission Cancel

- Grant System Admin privileges to the user you created, as shown in [Figure 29–18](#).

Figure 29–18 Grant New Permissions Pane with New User

Grant New Permissions

Permission Summary Grant New Permissions

Follow the steps below to grant new user or group permissions: Note, it is not possible to set permissions for "Anyone" or "Registered Users" here. To do this, use the Permissions Summary page.

- Choose the permissions: [\[select all\]](#)
 - System Admin
 - Category Admin
 - User Admin
 - Group Admin
 - Moderator
- Choose a user or group to grant the permissions to:
 - A Specific User: (enter username - separate multiple usernames with commas)
 - A Specific Group: (enter group name - separate multiple group names with commas)
- Done:

- Click **System > System Properties**.

The Jive Properties page displays (see [Figure 29–19](#)).

Figure 29–19 Jive Properties Page

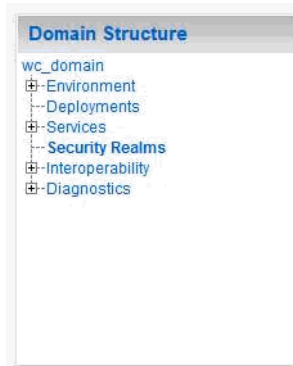
Jive Properties

Below is a list of system properties. Values for password-sensitive fields are hidden. Long property names and values have extra edit icon then look at the "Property Value:" field.

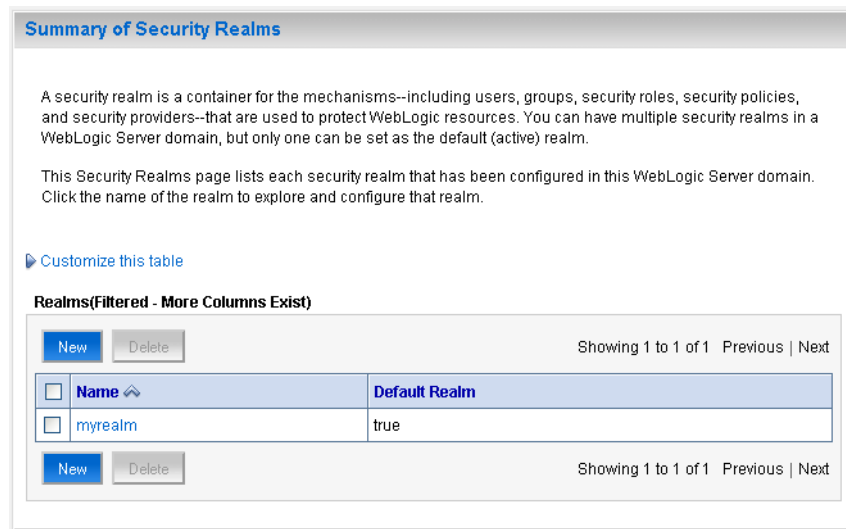
All Properties

Properties	
AuthFactory.className	= oracle.jive.security.JpsAuthFactory
cookieKey	= hidden
cron.propertiesUpgraded	= true
GroupManager.className	= oracle.jive.security.JpsGroupManager
locale.characterEncoding	= UTF-8
pwc_discussions.setup.complete_11.1.1.2.0	= true
UserManager.className	= oracle.jive.security.JpsUserManager
webservices.soap.custom.crypto.fileName	= crypto.properties
webservices.soap.custom.permissionHandler.className	= com.jivesoftware.webcenter.webservices.OraclePermissionHandler
webservices.soap.custom.wss4jHandler.className	= com.jivesoftware.webcenter.webservices.OracleHandlerProvider
webservices.soap.custom.xfire.active	= true

- Check that the properties marked in red have been added and are set as shown in [Figure 29–19](#).
- Log in to the WebLogic Server Administration Console.
For information on logging in to the WebLogic Server Administration Console, see [Section 1.13.2, "Oracle WebLogic Server Administration Console."](#)
- In the Domain Structure pane (see [Figure 29–20](#)), click **Security Realms**.

Figure 29–20 Domain Structure Pane

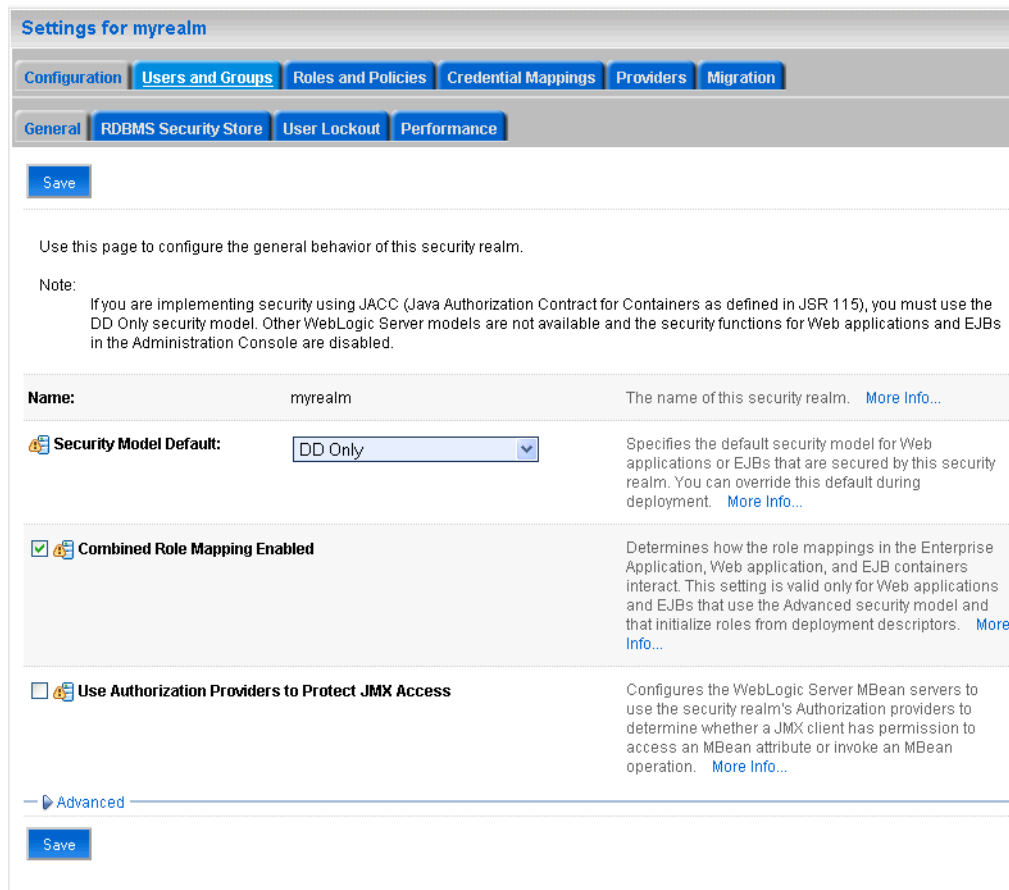
The Summary of Security Realms pane displays (see [Figure 29–21](#)).

Figure 29–21 Summary of Security Realms pane

- In the Name column, click the realm for which you want to change the administrator group name.

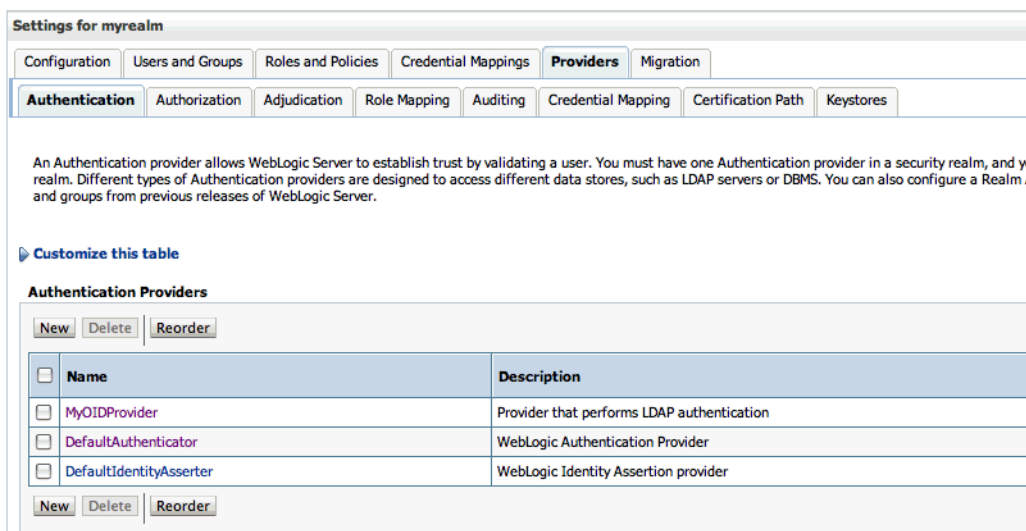
The Realm Settings pane displays (see [Figure 29–22](#)).

Figure 29–22 Realm Settings Pane



12. Select the Providers tab and the Authentication sub-tab, and reorder the authentication providers so that the authenticator for the external LDAP appears at the top of the list as shown in the example in Figure 29–23:

Figure 29–23 Providers Tab with Reordered Authentication Providers



13. Restart the domain Administration Server and discussions server.

29.5.2 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 must update the role definition for the WebLogic Server global Admin role using the WebLogic Server Administration Console.

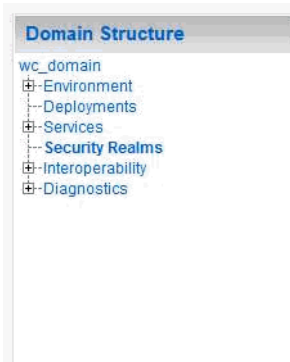
To update the role definition for the WebLogic Server global Admin role:

1. Log in to the WebLogic Server Administration Console.

For information on logging into the WebLogic Server Administration Console, see [Section 1.13.2, "Oracle WebLogic Server Administration Console."](#)

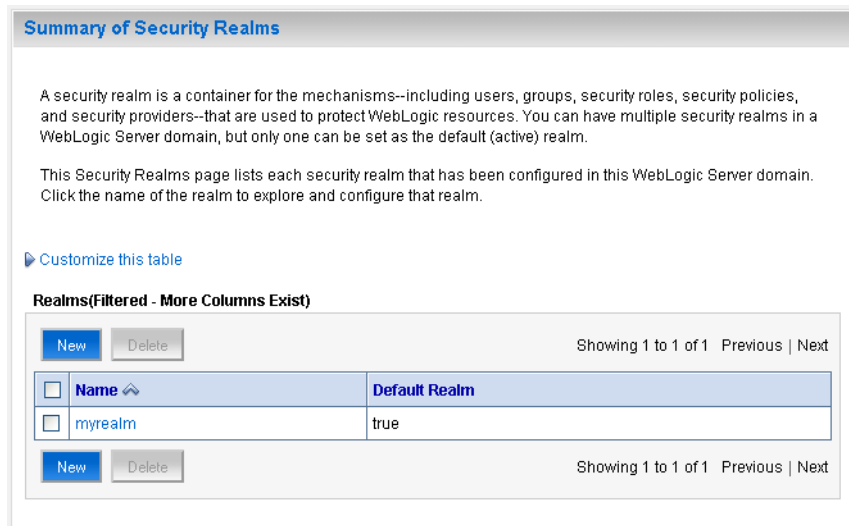
2. In the Domain Structure pane (see [Figure 29–24](#)), click **Security Realms**.

Figure 29–24 Domain Structure Pane



The Summary of Security Realms pane displays (see [Figure 29–25](#)).

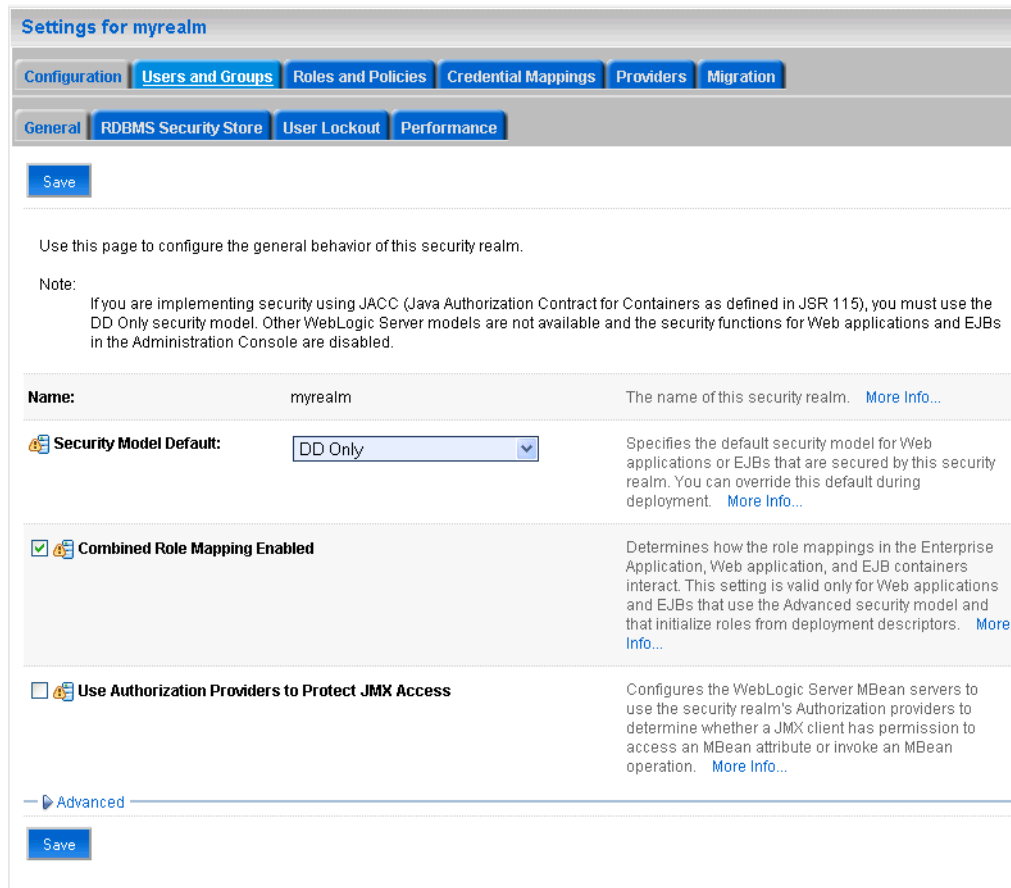
Figure 29–25 Summary of Security Realms pane



- In the Name column, click the realm for which you want to change the administrator group name.

The Realm Settings pane displays (see [Figure 29–26](#)).

Figure 29–26 Realm Settings Pane



- Open the Roles and Policies tab, and then the Realm Roles subtab.
The Realm Roles settings pane displays (see [Figure 29–27](#)).

Figure 29–27 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	View Role Conditions
AdminChannelUser	Global Role	View Role Conditions
Anonymous	Global Role	View Role Conditions
AppTester	Global Role	View Role Conditions
CrossDomainConnector	Global Role	View Role Conditions
Deployer	Global Role	View Role Conditions
Monitor	Global Role	View Role Conditions
Operator	Global Role	View Role Conditions
OracleSystemRole	Global Role	View Role Conditions
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 29–28](#)).

Figure 29–28 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 29–29](#)).

Figure 29–29 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 29–30](#)).

Figure 29–30 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 are authorized to administer WebLogic Server.

29.6 Configuring the Oracle Content Server to Share the Spaces Identity Store LDAP Server

Oracle Content Server (OCS) must be configured to use the same identity store LDAP server as Oracle Spaces. For more information on configuring the OCS, see [Chapter 11, "Managing Content Repositories"](#) and also "Configuring the LDAP Identity Store Service" in the *Oracle Fusion Middleware Application Security Guide*.

29.7 Aggregating Multiple Identity Store LDAP Servers Using libOVD

Sites with multiple identity stores can use libOVD to aggregate their user profile information. Two scenarios are covered in the step-by-step configuration instructions below:

- Users are available in distinct identity stores with complete user profile information available in the respective identity store.
- The same user is available in both identity stores with some attributes in one store and other attributes in the other store.

Note: If you are supporting self-registration with Active Directory, be sure to see the troubleshooting note in [Section 28.3.3, "Users Cannot Self-Register when Spaces Configured with Active Directory."](#)

This section contains the following subsections:

- [Section 29.7.1, "Configuring libOVD for Identity Stores with Complete User Profiles"](#)

- [Section 29.7.2, "Configuring libOVD for Identity Stores with Partial User Profiles"](#)
- [Section 29.7.3, "Restoring the Single Authenticator"](#)

29.7.1 Configuring libOVD for Identity Stores with Complete User Profiles

To configure libOVD where each identity store contains complete user profiles:

1. Create the required authenticators in the WLS Admin Console for the identity stores being configured and restart the Weblogic Admin and Managed Servers for the domain. Alternatively, you can also configure the identity store information in `jps-config.xml` by hand.
2. Update the identity store service instance in `jps-config.xml` and add a property `virtualize` with the value `true`. You can do this either by editing the `jps-config.xml` file by hand, or using Fusion Middleware Control.
3. WebCenter Portal lets users self-register, which creates a new user or group in the identity store. Since multiple identity stores are being used, you also need to explicitly specify the user create bases and group create bases in `jps-config.xml`. This step must be done by directly editing `jps-config.xml`.

The `jps-config.xml` file should look like the example below after the configuration.

```
<serviceInstance provider="idstore.ldap.provider" name="idstore.ldap">
  <property
    value="oracle.security.jps.wls.internal.idstore.WlsLdapIdStoreConfigProvider"
    name="idstore.config.provider" />
  <property value="oracle.security.idm.providers.stdlldap.JNDIPool"
    name="CONNECTION_POOL_CLASS" />
  <property value="true" name="virtualize" />
  <extendedProperty>
    <name>user.create.bases</name>
    <values>
      <value>ou=people,ou=myrealm,dc=wc_domain</value>
    </values>
  </extendedProperty>
  <extendedProperty>
    <name>group.create.bases</name>
    <values>
      <value>ou=groups,ou=myrealm,dc=wc_domain</value>
    </values>
  </extendedProperty>
</serviceInstance>
```

Be sure to replace the actual values for the user create base in "ou=people,ou=myrealm,dc=wc_domain" and group create base "ou=groups,ou=myrealm,dc=wc_domain."

29.7.2 Configuring libOVD for Identity Stores with Partial User Profiles

To configure libOVD where each identity store contains only partial user profiles:

1. Create the required authenticators in the WLS Admin Console for the identity stores being configured and restart the Weblogic Admin and Managed Servers for the domain. Alternatively, you can also configure the identity store information in `jps-config.xml` by hand.

2. Update the identity store service instance in `jps-config.xml` and add a property `virtualize` with the value `true`. You can do this either by editing the `jps-config.xml` file by hand, or using Fusion Middleware Control.
3. WebCenter Portal lets users self-register, which creates a new user or group in the identity store. Since multiple identity stores are being used, you also need to explicitly specify the user create bases and group create bases in `jps-config.xml`. This step must be done by directly editing `jps-config.xml`.

The `jps-config.xml` file should look like the example below after the configuration.

```
<serviceInstance provider="idstore.ldap.provider" name="idstore.ldap">
<property
value="oracle.security.jps.wls.internal.idstore.WlsLdapIdStoreConfigProvider"
name="idstore.config.provider"/>
<property value="oracle.security.idm.providers.stldap.JNDIPool"
name="CONNECTION_POOL_CLASS"/>
<property value="true" name="virtualize"/>

<extendedProperty>
  <name>user.create.bases</name>
  <values>
    <value>ou=people,ou=myrealm,dc=wc_domain</value>
  </values>
</extendedProperty>
<extendedProperty>
  <name>group.create.bases</name>
  <values>
    <value>ou=groups,ou=myrealm,dc=wc_domain</value>
  </values>
</extendedProperty>
</serviceInstance>
```

In the above example "ou=people,ou=myrealm,dc=wc_domain" and "ou=groups,ou=myrealm,dc=wc_domain" are the user and group create bases respectively. The actual values should be substituted while doing the configuration.

4. Run the following OVD WLST commands to configure the Join Adapter for the identity stores. Go to `$MWHOME/oracle_common/common/bin` and invoke `wlst.sh` (`wlst.cmd` in windows) and bring up the WLST prompt. Connect to the Weblogic Administration Server and run the following WLST commands.

```
createJoinAdapter(adapterName="<Join Adapter Name>", root="<Namespace>",
primaryAdapter="<Primary adapter Name>")
```

```
addJoinRule(adapterName="<Join Adapter Name>", secondary="<Secondary Adapter
Name>", condition="<Join Condition>")
```

If there are more secondary identity stores, then run the `addJoinRule` command for each secondary identity store.

```
modifyLDAPAdapter(adapterName="<AuthenticatorName>", attribute="Visible",
value="Internal")
```

Run the above `modifyLDAPAdapter` command for each identity stores that is configured.

Example**Authenticator 1:**

In this example, the same user is available in both identity stores with some attributes in one store and some in the other. For this example, AD is the primary store and OID is the secondary store.

Authenticator Name: AD

User Base: cn=users, dc=acme, dc=com

Authenticator 2:

Authenticator Name: OID

User Base: cn=users, dc=oid, dc=com

Perform steps 1 - 3 above, specifying the `user.create.bases` and `group.create.bases` corresponding to the primary adapter's namespace.

Perform the following WLST commands:

```
createJoinAdapter(adapterName="JoinAdapter1", root="dc=acme,dc=com",
primaryAdapter="AD")
addJoinRule(adapterName="JoinAdapter1", secondary="OID", condition="uid=cn")
```

"uid=cn" is the join condition in the above example, which indicates that if the `uid` value of a user in the secondary identity store (OID) matches with the `cn` value of the user in the primary identity store (AD), then the attributes will be combined.

```
modifyLDAPAdapter(adapterName="OID", attribute="Visible", value="Internal")
modifyLDAPAdapter(adapterName="AD", attribute="Visible", value="Internal")
```

Restart the WebLogic Administration server and Managed Servers.

29.7.3 Restoring the Single Authenticator

You can restore the single authenticator by removing the Join Adapter rule, thereby backing out the configuration done in [Section 29.7.2, "Configuring libOVD for Identity Stores with Partial User Profiles."](#)

To remove the Join Adapter rule, connect to the Weblogic Administration Server and run the following WLST commands:

```
deleteAdapter(adapterName="JoinAdapter1")
modifyLDAPAdapter(adapterName="oid auth", attribute="Visible", value="Yes")
modifyLDAPAdapter(adapterName="AD", attribute="Visible", value="Yes")
```

Restart the WebLogic Administration server and Managed Servers and make sure that users from both identity stores are able to log in.

29.8 Configuring Dynamic Roles for the Spaces Application

This section describes how to configure dynamic roles for Spaces.

This section contains the following subsections:

- [Section 29.8.1, "Overview of Configuring Dynamic Roles"](#)
- [Section 29.8.2, "Prerequisites to Configuring Dynamic Roles"](#)
- [Section 29.8.3, "Installing the OVD Plug-in"](#)
- [Section 29.8.4, "Configuring Dynamic Roles"](#)

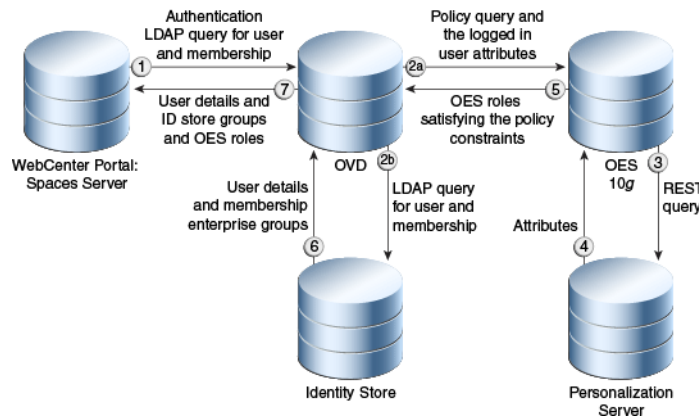
29.8.1 Overview of Configuring Dynamic Roles

With static roles, the role to membership relationship is static. This relationship is established at provisioning time, and once established, and after a user logs in, the subject is populated with all the roles for which the user is a direct member or indirectly a member based on an enterprise group.

Dynamic roles provide for rule-based role membership. Membership to an application role is provided through a dynamic group. Dynamic group definitions can include constraints for user profile attributes, and date and time that provide a flexible way to provide access to an application. For example, a user could be allowed to access an application only during their shift or during maintenance periods without explicitly having to grant them that access. Note that rules based on session or request attributes are not supported in this release.

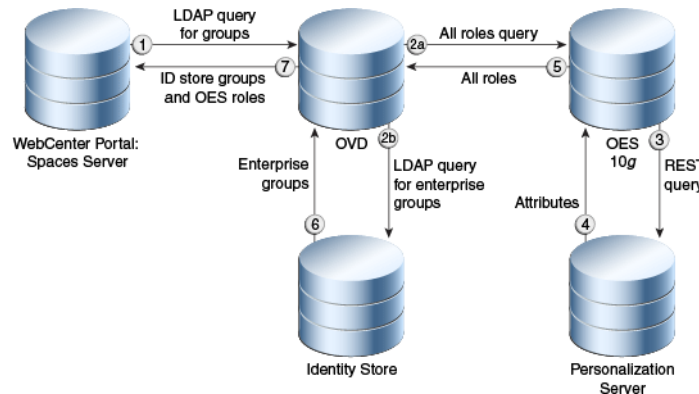
Dynamic roles can be defined in Oracle Entitlement Server (OES) 10g as a role with constraints. The role defined in OES is added to user's enterprise group principal through an OVD plug-in. When the user logs in the policy rules are evaluated to determine whether the user's subject gets the dynamic group principal. [Figure 29-31](#) shows the login process for a topology configured with OES and the OVD plug-in.

Figure 29-31 Login Process



[Figure 29-32](#) shows what happens during a dynamic group query for a topology configured with OES and the OVD plug-in.

Figure 29-32 Group Query



29.8.2 Prerequisites to Configuring Dynamic Roles

Prior to installing and configuring the OVD plug-in, you should already have installed and configured Oracle Internet Directory (OID), Oracle Virtual Directory (OVD) 11g, and Oracle Entitlement Server (OES) 10g. Note that the OVD plug-in is not currently certified with OES 11g.

OID and OVD are part of the Oracle Identity Management 11g suite. If you have not already installed them, install them as described in "Installing and Configuring Oracle Identity Management (11.1.1.6.0)" in *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*. Configure OVD by running `config.sh` as described in the section "Configuring Oracle Virtual Directory (OVD)" in *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

Install OES with RMI-SSM and the latest cumulative patch as described in the section "Configuring a Remote SSM and Proxy" in the *SSM Installation and Configuration Guide*.

Additionally, if you have plan to incorporate constraints based on Personalization for WebCenter Portal, you will also need to install and configure the Personalization server, as described in [Chapter 20, "Managing Personalization for WebCenter Portal."](#)

29.8.3 Installing the OVD Plug-in

Oracle Virtual Directory (OVD) is a part of the Oracle Identity Management suite of products. OVD provides an elegant solution to the problem of integrating multiple heterogeneous data sources presenting them as a consolidated view that can be consumed by an LDAP client in WebCenter Portal. Through OVD, OES data can be exposed by means of an OVD custom adaptor in a way that it can be consumed by Spaces. The adapter can represent non-LDAP data as an LDAP-like tree hierarchy. The functionality of the custom adapter is contained in a plug-in that can be attached to the adapter.

To install the OVD plug-in:

1. Download the `oes-ovd-plugin.zip` file from:

```
http://download.oracle.com/otndocs/tech/webcenter/files/oes-ovd-plugin.zip
```

2. Make a copy of the `oes-ovd-plugin.zip` file.
3. Go to the `plugins/lib` directory where OVD was installed (for example, `asinst_1/OVD/ovd1/plugins/lib`).
4. Unzip `oes-ovd-plugin.zip`.
5. Copy `webcenterNames.xml` to the instance home (for example, `<ORACLE_HOME>/asinst_1`).
6. Create the following directories:

```
mkdir pdpproxy
mkdir keys
```

7. Copy the following OES jars from the `OES/rmi-ssm` installation directory to the `lib` directory:

```
EccpressoCore.jar
antlr.jar
api.jar
asi_classes.jar
asitools.jar
commons-pool-1.3.jar
connector.jar
```

```

framework.jar
jsafeFIPS.jar
jsafeJCEFIPS.jar
kodo-runtime.jar
log4j.jar
managementapi.jar
orawsdl14.jar
rmi-ssm.jar
rmi-stubs.jar
rmi-types.jar
ssladapter.jar
sslplus.jar
webservice.jar
webserviceclient.jar
webservices.jar
xbean.jar

```

8. Go to the `keys` directory that you just created and copy all the keys in the OES install (`ales32-shared/keys` directory) here.
9. Go to the `pdproxy` directory that you just created and copy the PDP configuration properties file from OES (`rmi-ssm/pdproxy/PDPProxyConfiguration.properties`).
10. Restart the OVD process with the following command:


```
./opmnctl stopall startall
```
11. If you are planning to use Personalization in defining your constraints, install the `p13nattributeRetriever` as shown below:
 - a. Locate the `<WebCenter Home>/webcenter/modules/oracle.webcenter.framework_11.1.1/attribute-retriever.jar` file.
 - b. Locate the `rmi-ssm/lib/providers` directory of the OES installation, and copy the `attribute-retriever.jar` file there.
 - c. Restart the `rmi-ssm`.

29.8.4 Configuring Dynamic Roles

This section describes how to configure your Spaces environment to support dynamic roles through OES and the OVD plug-in. Prior to completing the configuration steps in this section, you should already have installed the prerequisite applications (described in [Section 29.8.2, "Prerequisites to Configuring Dynamic Roles"](#)) and the OVD plug-in (described in [Section 29.8.3, "Installing the OVD Plug-in"](#)).

This section contains the following subsections:

- [Section 29.8.4.1, "Configuring OES"](#)
- [Section 29.8.4.2, "Configuring the OVD Plug-in"](#)
- [Section 29.8.4.3, "Configuring the Personalization Attributes"](#)
- [Section 29.8.4.4, "Configuring the Spaces Application to Consume Dynamic Roles"](#)

29.8.4.1 Configuring OES

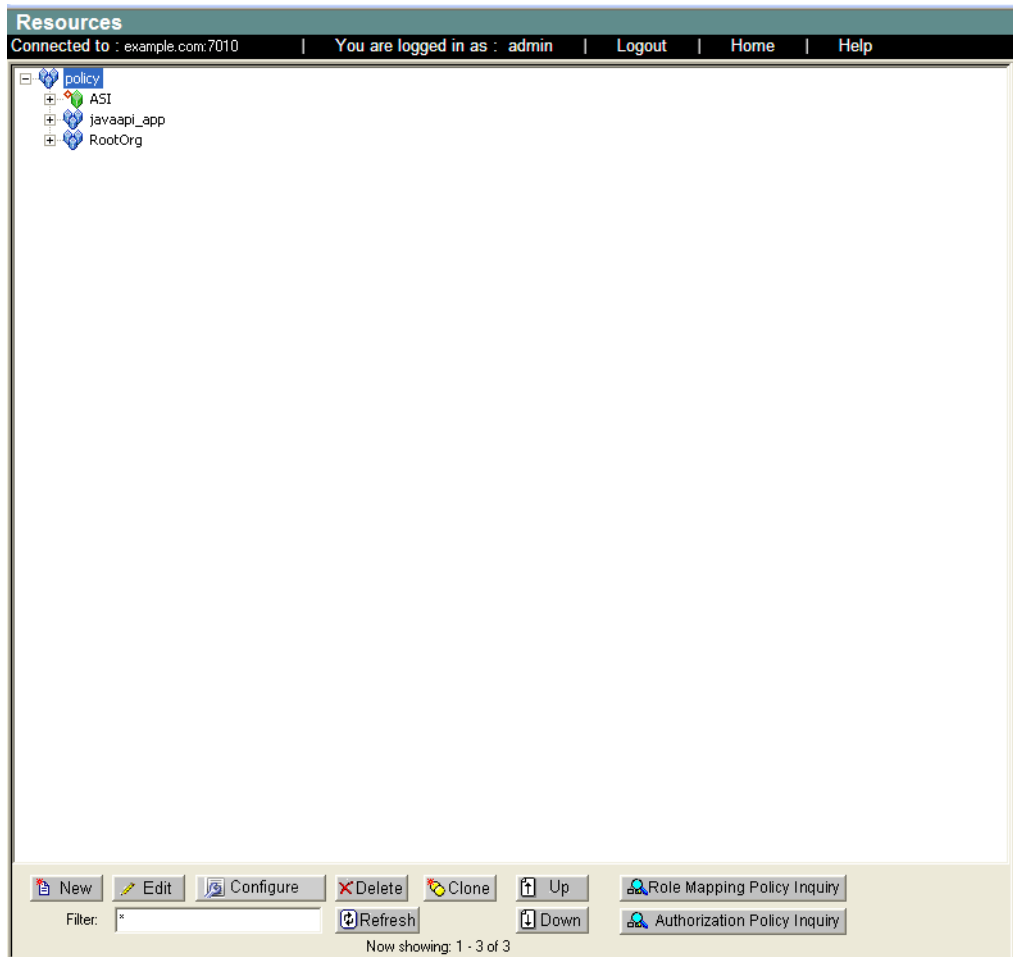
All the dynamic roles that you want to be available in Spaces should be defined under a single umbrella resource and action. In the steps below, we're using `WebCenterApp/WebCenterResource` as the umbrella resource, and `browse` as the

action. When you create the dynamic roles, the roles are then granted browse permission on the resource using role mapping policies. A role mapping policy can also have additional constraints based on identity store or Personalization attributes.

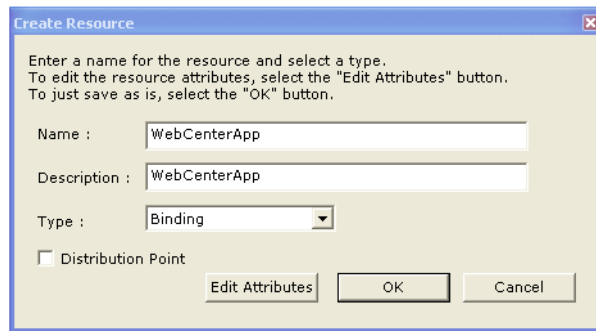
To configure OES for dynamic groups:

1. Open a browser and log onto the OES console as an administrator:
`https://<host>:<port>/asi`
2. Under the Administration Console node, click **Resources** to display a list of the currently defined resources in the Resources page as shown in [Figure 29–33](#).

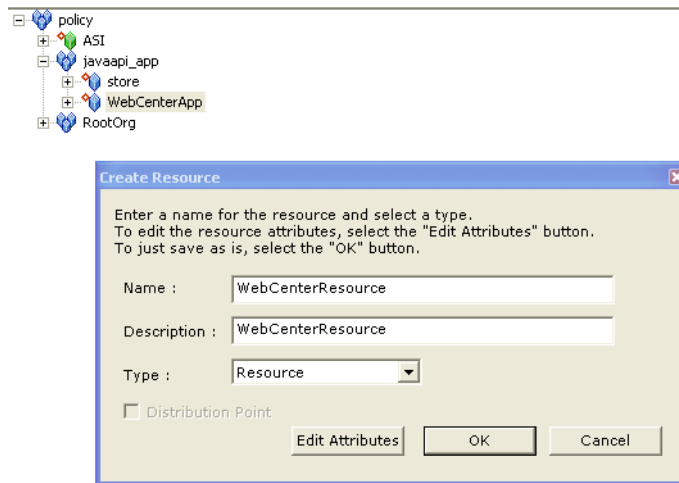
Figure 29–33 Resources Page



3. Create a resource root by right-clicking the `javaapi_app` node and selecting **Add Resource** to display the Create Resource dialog. Name the resource `WebCenterApp` and select **Binding** as the **Type** as shown in [Figure 29–34](#).

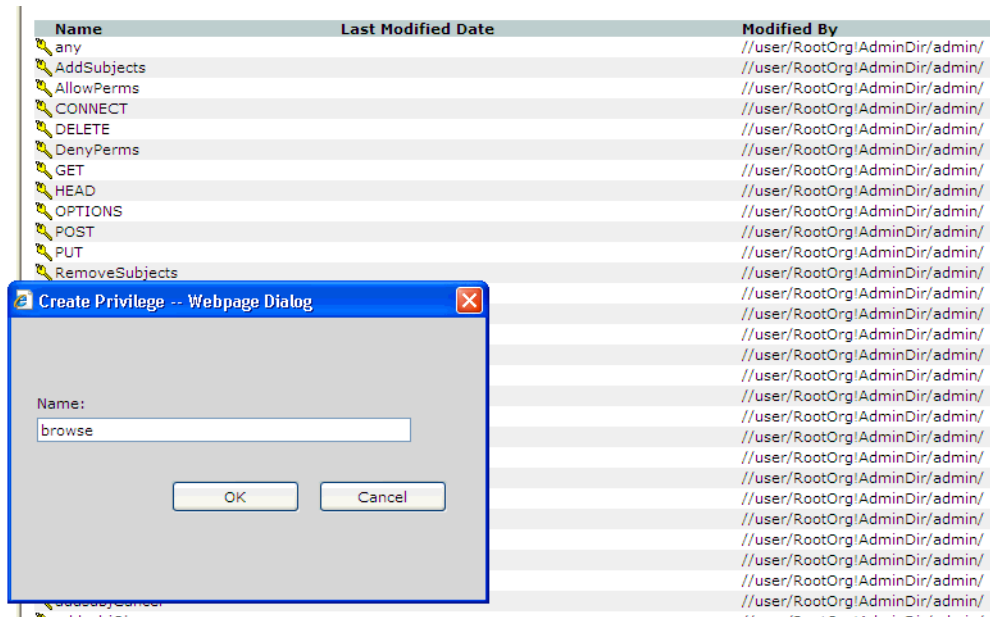
Figure 29–34 Creating a Root Resource

4. Right-click `WebCenterApp` and create a new resource under it naming it `WebCenterResource` and selecting `Resource` as the **Type** as shown in [Figure 29–35](#).

Figure 29–35 Creating a Resource

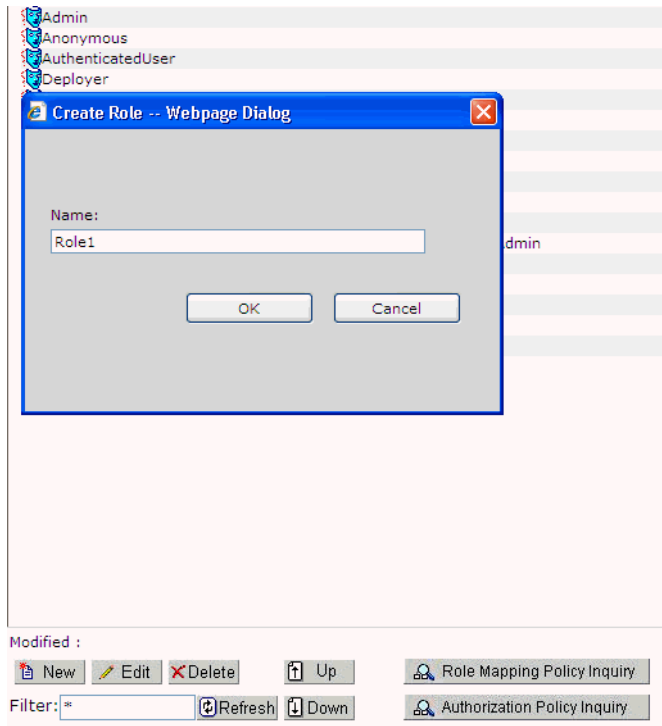
5. Under the Resources node, click **Privileges** to display the Privileges page.
6. Click **New** and create an action naming it `browse` as shown in [Figure 29–36](#).

Figure 29–36 Creating an Action



7. Open the Identity node and click **Roles** to display the Roles page.
8. Click **New** to create the dynamic roles using the Create Role dialog as shown in Figure 29–37.

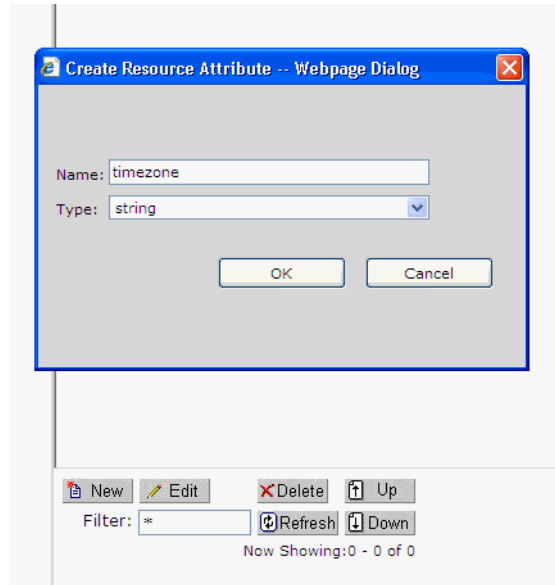
Figure 29–37 Creating the Dynamic Roles



9. Open the Resources node and click **Attributes** to display the Resource Attributes page.

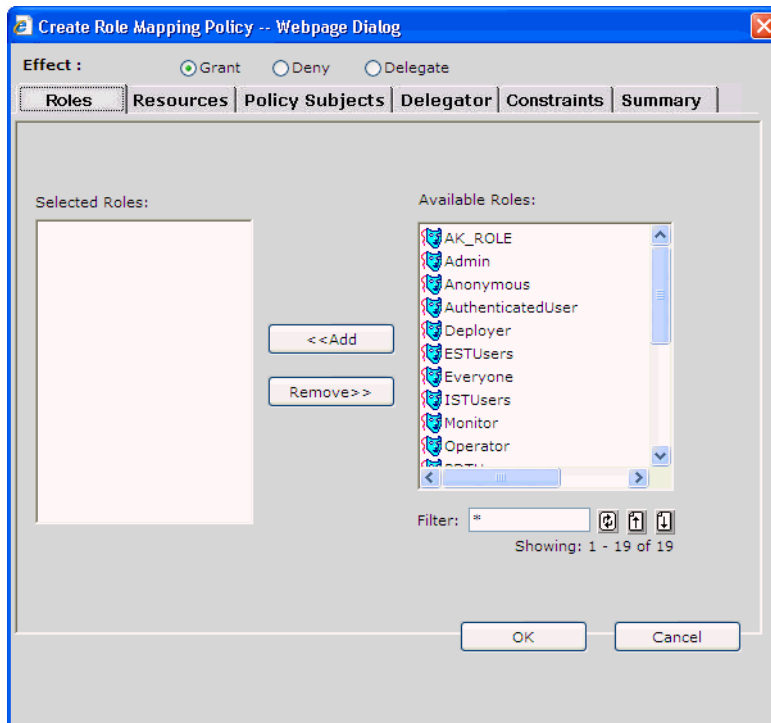
10. Click **New** and use the Create Resource Attribute dialog to create resource attributes using the same name as the identity store attributes that are to be used in the constraints (for example, `business_email` or `timezone`) as shown in [Figure 29–38](#). If Personalization attributes are to be used in the constraints then those attributes should also be created.

Figure 29–38 *Creating Resource Attributes*



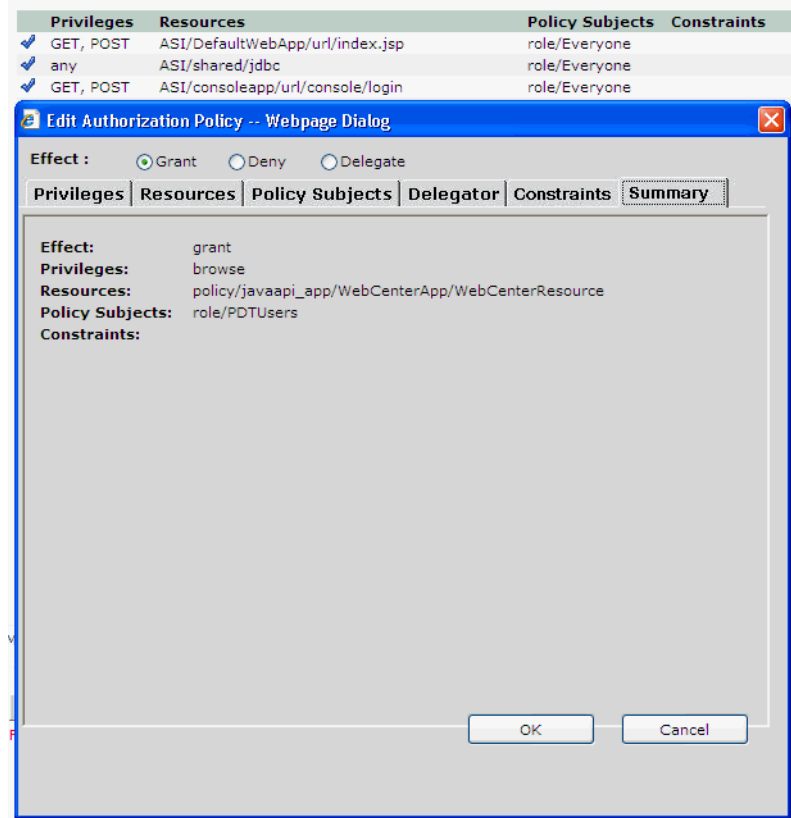
11. Open the Policy node and click **Role Mapping Policies** to display the Role Mapping Policies page.
12. Click **New** to display the Create Role Mapping Policy dialog and create role mapping policies and constraints using the identity store attributes or built-in system attributes (such as `hour` or `day`) as shown in [Figure 29–39](#).

Figure 29–39 Creating Role Mapping Policies



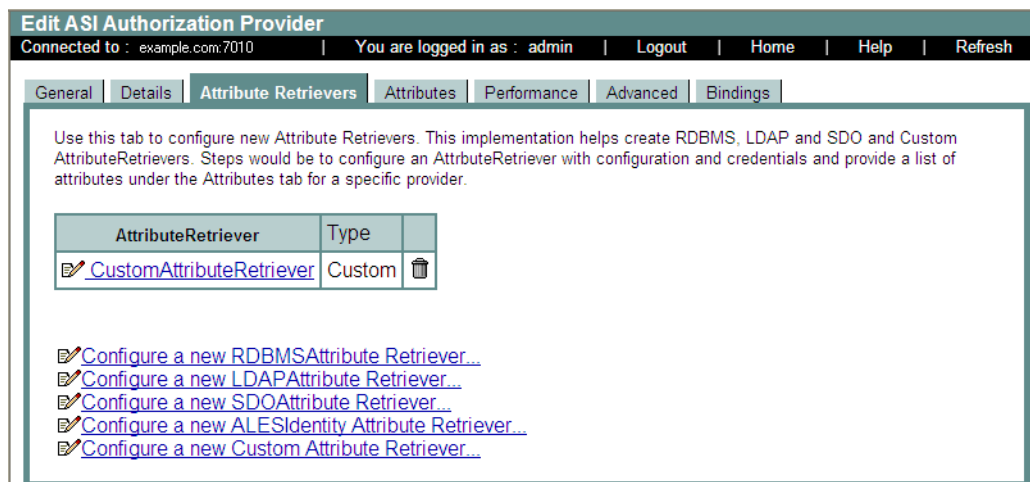
13. Under the Policy node click **Authorization Policies** to display the Authorization Policies page.
14. Click New to use the Create Authorization Policies dialog to create new authorization policies, or from the summary of authorization policies select a policy and click **Edit** to edit and provide details for the policy such resources and policy subjects as shown in [Figure 29–40](#).

Figure 29–40 Creating Authorization Policies



- Open the Authorization node under Service Control Managers, click **ASIAuthorizationProvider** and then open the Attribute Retrievers tab as shown in Figure 29–41.

Figure 29–41 Attribute Retrievers Tab



- Click **Configure a new Custom Attribute Retriever** and create a custom attribute retriever named `WebCenterP13nAttributeRetriever` (`oracle.webcenter.security.internal.plugins.oes.attributeretr`

iever.WebCenterP13nAttributeRetriever), adding the class details as shown in [Figure 29–42](#).

Figure 29–42 Creating a Custom Attribute Retriever

Custom Attribute Retriever

Name:

Name

Attribute Retriever Type: Custom

Type of the Attribute Retriever.

Attribute Retrievers:

Specifies comma separated list of plugins used to retrieve attribute values from complex data objects. These classes should implement the AttributeRetriever interface.

Cache All Attributes

Cache all Attributes for this retriever. If individual attributes is configured using the Attributes tab, then the attribute cache setting over ride this setting.

Cache All Attributes TTL:

The duration for which to cache data, in seconds. Attribute TTLs settings if configured, over ride this setting.

- Open the Role Mapping node under Service Control Managers, click **ASIRoleMapperProvider** and open the Bindings tab. Bind the WebCenterApp resource to the authorization provider as shown in [Figure 29–43](#).

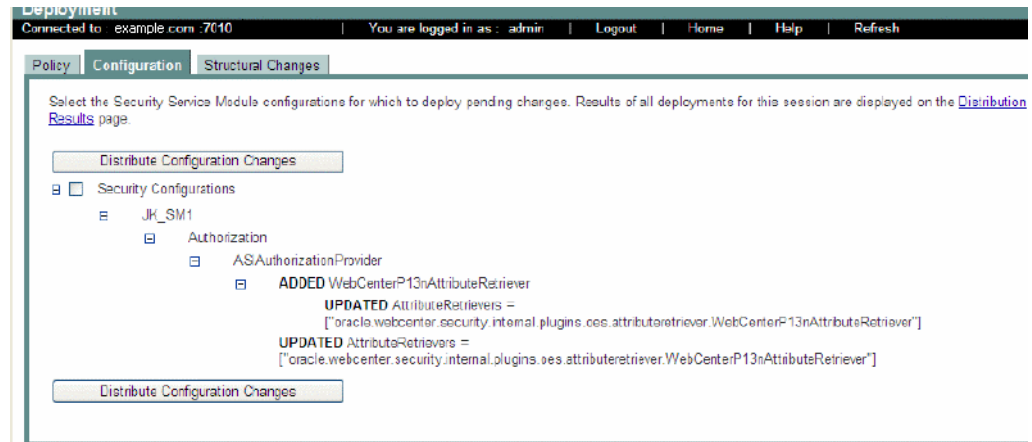
Figure 29–43 Binding the Resource to the Authorization Provider

General | Details | Performance | Advanced | **Bindings**

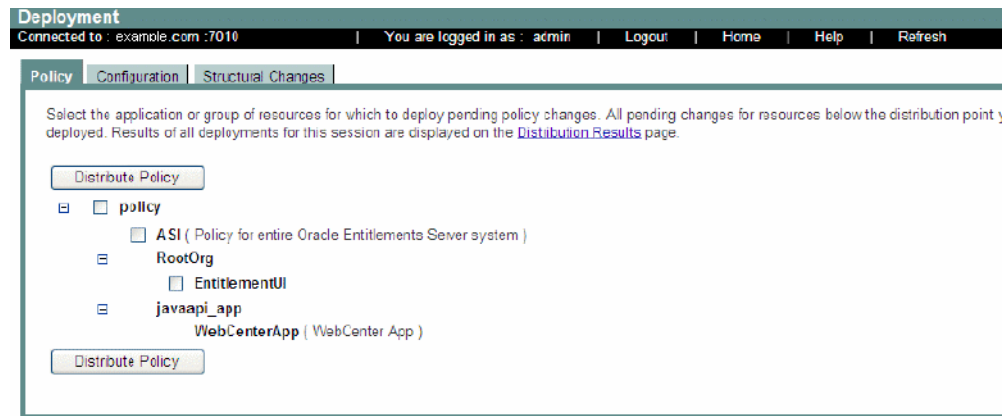
Use this tab to bind a resource to this provider. The ASI Authorization and ASI Role Mapper providers for a Security Service Module only enforce policies for a subset of the resources. Binding applications to the provider determines the subset of those resources. The Security Service Module can only protect resources that are bound to it. A resource is bound to only one Security Service Module and ASI Authorization and ASI Role Mapper provider. The resources you bind must be the same for both providers

Resource Name
//app/policy/javaapi_app/store

- Click **Deployment**, open the Configuration tab and distribute the configuration changes as shown in [Figure 29–44](#).

Figure 29–44 Distributing the Configuration Changes

19. Open the Policy tab and distribute the policy changes as shown in [Figure 29–45](#).

Figure 29–45 Distributing the Policy Changes

29.8.4.2 Configuring the OVD Plug-in

This section describes how to configure the OVD plug-in.

To configure the OVD plug-in:

1. Go to the `plugins/lib/pdpproxy` directory and edit the file `PDPProxyConfiguration.properties`, providing the SSM configuration ID, the OES host name, the RMIS port, and the trust store location. Example values are shown below:

```
SSMConfigID=JK_SM1
PDPTransport=RMI
PDPAddress=rmis://example.com:9300 (the use of SSL port is always recommended)
TrustStore=<OID_HOME>/asinst_1/OVD/ovd1/plugins/lib/keys/DemoTrust.jks
```

2. Open the file `./config/OPMN/opmn/opmn.xml` and change the `java-options` and `java-classpath` of the OVD process shown in the following sample, providing the correct OVD home path:

```
<data id="java-options" value="-server -Xms256m -Xmx256m
-Dvde.soTimeoutBackend=0 -Didm.oracle.home=$ORACLE_HOME
-Dcommon.components.home=$ORACLE_HOME/../../oracle_common
-Doracle.security.jps.config=$ORACLE_INSTANCE/config/JPS/jps-config-jse.xml
```

```
-Djavax.net.ssl.trustStore=$ORACLE_INSTANCE/OVD/ovd1/plugins/lib/keys/DemoTrust
.jks
-Dpdp.configuration.properties.location=$ORACLE_INSTANCE/OVD/ovd1/plugins/lib/p
dpproxy/PDPProxyConfiguration.properties -Dwles.ssl.identityKeyAlias=wles-admin
-Dwles.ssl.identityKeyPasswordAlias=wles-admin
-Dwles.ssl.identityKeyStore=$ORACLE_INSTANCE/OVD/ovd1/plugins/lib/keys/identity
.jceks
-Dwles.ssl.trustedCAKeyStore=$ORACLE_INSTANCE/OVD/ovd1/plugins/lib/keys/trust.j
ks
-Dwles.ssl.passwordFile=$ORACLE_INSTANCE/OVD/ovd1/plugins/lib/keys/password.xml
-Dwles.ssl.passwordKeyFile=$ORACLE_INSTANCE/OVD/ovd1/plugins/lib/keys/password.
key" />
```

```
<data id="java-classpath"
value="$ORACLE_INSTANCE/OVD/ovd1/plugins/lib/jsafeFIPS.jar:
$ORACLE_INSTANCE/OVD/ovd1/plugins/lib/jsafeJCEFIPS.jar:
$ORACLE_INSTANCE/OVD/ovd1/plugins/lib/scmapi.jar:
$ORACLE_INSTANCE/OVD/ovd1/plugins/lib/sslplus.jar:
$ORACLE_INSTANCE/OVD/ovd1/plugins/lib/ssladapter.jar:
$ORACLE_INSTANCE/OVD/ovd1/plugins/lib/asitools.jar:
$ORACLE_INSTANCE/OVD/ovd1/plugins/lib/webserviceclient.jar:
$ORACLE_INSTANCE/OVD/ovd1/plugins/lib/EccpressoCore.jar:
$ORACLE_INSTANCE/OVD/ovd1/plugins/lib/webservice.jar:
$ORACLE_INSTANCE/OVD/ovd1/plugins/lib/kodo-runtime.jar:
$ORACLE_INSTANCE/OVD/ovd1/plugins/lib/kodo-runtime.jar:
$ORACLE_INSTANCE/OVD/ovd1/plugins/lib/commons-pool-1.3.jar:
$ORACLE_INSTANCE/OVD/ovd1/plugins/lib/oes-ovd-plugin.jar:
$ORACLE_INSTANCE/OVD/ovd1/plugins/lib/xbean.jar:
$ORACLE_INSTANCE/OVD/ovd1/plugins/lib/antlr.jar:
$ORACLE_INSTANCE/OVD/ovd1/plugins/lib/log4j.jar:
$ORACLE_INSTANCE/OVD/ovd1/plugins/lib/api.jar:
$ORACLE_INSTANCE/OVD/ovd1/plugins/lib/asi_classes.jar:
$ORACLE_INSTANCE/OVD/ovd1/plugins/lib/framework.jar:
$ORACLE_INSTANCE/OVD/ovd1/plugins/lib/rmi-types.jar:
$ORACLE_INSTANCE/OVD/ovd1/plugins/lib/rmi-ssm.jar:
$ORACLE_HOME/ovd/jlib/vde.jar$: $ORACLE_HOME/jdbc/lib/ojdbc6.jar" />
```

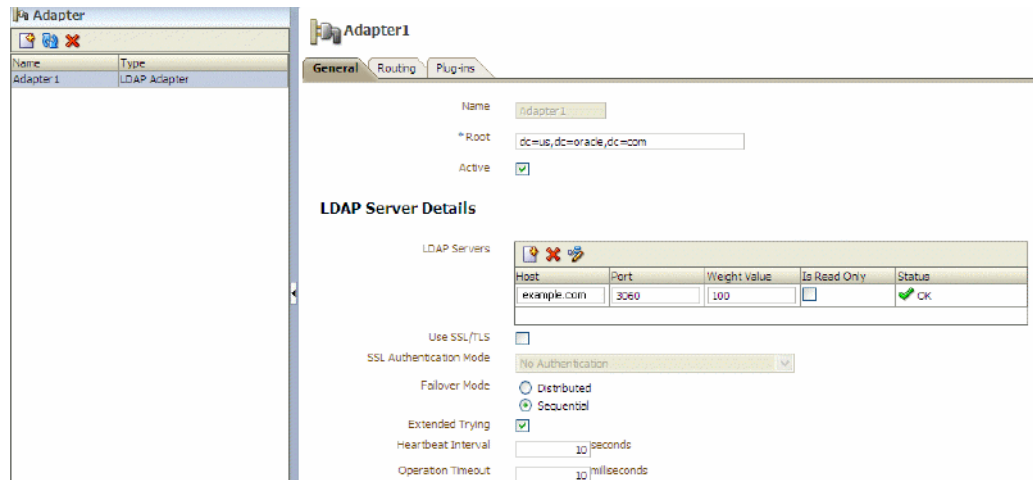
3. Using your browser, open the Oracle Directory Service Manager (ODSM):

```
http://host:port/odsm
```

To determine the ODSM port use the `opmnctl status` command in the OID installation. The default port is 7005.

4. Create an adapter of **Type** `LDAP Adapter`, providing the LDAP host and port details as shown in the example in [Figure 29-46](#).

Figure 29–46 Example LDAP Adapter



5. Choose the DN and provide a mapping name for the DN.
6. If you need to map to attributes other than the default, open the Plug-ins tab of the adapter and add the UserManagement adapter. For example, if you are using Active Directory as the backend directory server for OVD, add the UserManagement adapter providing the following parameter mappings:

```
<param name="directoryType" value="ActiveDirectory" />
<param name="mapAttribute" value="orclguid=objectguid" />
<param name="mapAttribute" value="cn=sAMAccountName" />
<param name="mapAttribute" value="uniquemember=member" />
<param name="mapAttribute" value="OESRole=OESRole" />
<param name="mapObjectclass" value="orclGroup=group" />
<param name="mapObjectclass" value="groupofurls=group" />
<param name="mapObjectclass" value="groupofuniquenames=group" />
<param name="mapObjectclass" value="person=user" />
<param name="mapRDNAttribute" value="uniquemember=member" />
```

For more information about configuring the UserManagement adapter, see "UserManagement Plug-In" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.

7. Add the OES10gUserEntitlementsPlugin and add all the plug-in parameters as shown in the example below, replacing the host and port details for BLM and Personalization (p13n) for your local environment:

```
<param name="ldap_group_basedn" value="cn=Groups,dc=us,dc=oracle,dc=com" />
<param name="ldap_user_basedn" value="cn=Users,dc=us,dc=oracle,dc=com" />
<param name="ldap_admin_user" value="cn=Administrator" />
<param name="oes_admin_user" value="admin" />
<param name="OrclOVDEncrypted_oes_admin_pass" value="<password>" />
<param name="oes_config_name" value="JK_SM1" />
<param name="oes_policy_domain" value="JK_SM1" />
<param name="oes_resource_action" value="browse" />
<param name="oes_resource_name" value="WebCenterApp/WebCenterResource" />
<param name="oes_resource_namespace" value="webcenterResource" />
<param name="oes_roles_cache_interval" value="180000" />
<param name="oes_action_namespace" value="webcenterAction" />
<param name="p13n_admin_user" value="weblogic" />
<param name="OrclOVDEncrypted_p13n_admin_pass" value="<password>" />
<param name="oes_blm_host" value="example.com" />
<param name="oes_blm_port" value="7011" />
```

```

<param name="oes_p13n_index_url" value="example.com"/>
<param name="oes_p13n_prop_url" value="example.com"/>
<param name="ldap_eqmatch" value="equalityMatch"/>
<param name="ldap_loginattr" value="sAMAccountName"/>
<param name="ldap_loginattr" value="mail"/>
<param name="ldap_loginattr" value="cn"/>

```

Note that passwords, once entered as plug-in parameters, are encrypted and then stored on the server.

- Restart the OVD process using the following command:

```
./opmnctl stopall startall
```

Make sure that the OVD process restarts without any exceptions before continuing. If you encounter errors, you can turn on logging in the plug-in, by adding the following entry to:

```

<INSTANCE_HOME>/config/OVD/ovd1/ovd-logging.xmlovd-logging.xml

<logger name='oracle.webcenter.security.internal.plugins.ovd' level='TRACE:1'
useParentHandlers='false'>
    <handler name='OVDHandler' />
</logger>

```

- If SSL-enabled Personalization attributes are required, then import the certificate containing the public key of the Personalization server into the trust store on OVD, which is typically the JDK's `cacerts` file.

29.8.4.3 Configuring the Personalization Attributes

If you are using Personalization attributes as part of your constraints, then follow the instructions in "Viewing a Property Set Within a Namespace Using the Property Service" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal* to configure them. For more information about Personalization for WebCenter Portal, see [Chapter 20, "Managing Personalization for WebCenter Portal."](#)

29.8.4.4 Configuring the Spaces Application to Consume Dynamic Roles

This section describes how to prepare Spaces to consume dynamic roles defined in OES 10g.

By default, Spaces picks up only the static enterprise roles defined in the identity store. To use the dynamic roles defined within OES (Oracle Entitlements Server), you need to add the OVD plug-in as the authenticator. The OVD plug-in can then consolidate the static roles from the identity store and the dynamic roles from OES.

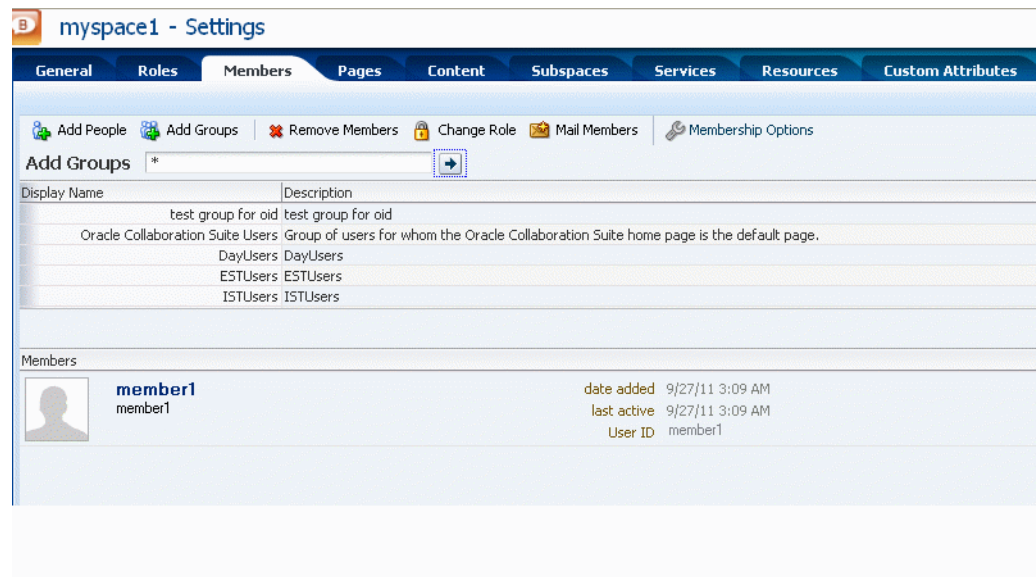
To configure Spaces to consume dynamic roles:

- Log in to the WebLogic Server Administration Console.
For information on logging into the WebLogic Server Administration Console, see [Section 1.13.2, "Oracle WebLogic Server Administration Console."](#)
- Add an authenticator of **Type** Oracle Virtual Directory providing the OVD connection details, and the group base dn and user base dn.
Leave the rest of the settings as their default values. Any directory-specific mapping should be done only in the adapter using the UserManagement plug-in. For more information about configuring the UserManagement adapter, see "UserManagement Plug-In" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.

3. Restart all servers.
4. Log onto Spaces as a user in OID and create a group space.
5. Go to **Add Members > Groups > Search** and add the enterprise roles you want as members to a group space as shown in [Figure 29–47](#).

With OVD as the authenticator, you should see both dynamic (from OES) and static groups. In [Figure 29–47](#), the dynamic groups are `ESTUsers`, `DayUsers` and `ISTUsers`, with the rest being static groups from OID.

Figure 29–47 Adding Static and Dynamic Groups to a Space



29.9 Configuring Dynamic Groups for the Spaces Application

A dynamic group is a static group that is dynamically populated. Dynamic groups can be assigned to roles and used within Spaces in the same way as static groups.

Within the application, Spaces does not distinguish between static and dynamic groups. Dynamic groups are configured entirely in the identity store (and their configuration is specific to the LDAP implementation being used), and exposed in the same manner as static groups (in fact a dynamic group can be a composite of a static member list and a dynamically determined membership).

The dynamic membership of the group is defined by setting the group's `labeledURI` attribute with an appropriate LDAP query filter. The query filter defines the set of users that will define the membership of the group.

For Oracle Internet Directory, you can create a dynamic group with an LDIF file and using the `ldapadd` command, or using the Oracle Directory Services Manager (ODSM). These two options are described in the following subsections:

- [Section 29.9.1, "Creating a Dynamic Group Using an LDIF File"](#)
- [Section 29.9.2, "Creating a Dynamic Group Using the Oracle Directory Services Manager"](#)

29.9.1 Creating a Dynamic Group Using an LDIF File

To create the dynamic group using an LDIF file:

1. Create an LDIF file with a text editor. The following example shows how a dynamic group can be defined that represents all users under the default user search base, with the title of "Manager":

Example 29–1 Defining a Dynamic Group Using an LDIF File

```
dn:
cn=managers,cn=portal.070720.104824.056918000,cn=groups,dc=us,dc=oracle,dc=com
labeleduri: ldap://myserver.example.com:12061/cn=users,dc=us,dc=mybiz,dc=com
??sub?(title=Manager)
description: Dynamic Group of Managers
cn: Managers
orclisvisible: true
objectclass: orclDynamicGroup
objectclass: orclGroup
objectclass: top
objectclass: groupOfUniqueNames
displayname: Managers
owner: cn=fmwadmin,cn=users,dc=us,dc=mybiz,dc=com
```

Note: The labeledURI syntax for an LDAP URL is defined in RFC 2255 (<http://www.faqs.org/rfcs/rfc2255.html>). In the example above, it is representing a search for any entry under the DN `cn=users,dc=us,dc=mybiz,dc=com` with the attribute `title=Manager`. This is to be done on the server `myserver.example.com` at LDAP port 12061 and using a subtree ("sub") search.

A dynamic group can be defined on any attribute or condition that can be represented as an LDAP URL and defined in the `labeledURI` attribute. Dynamic groups can also be defined using the `ConnectBy` assertion, which is included in the `orclDynamicGroup` objectClass. Refer to the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* for more information for this alternate approach.

2. Save the file, and then update the OID server by issuing the `ldapadd` command. For example:

Example 29–2 Updating OID Using the `ldapadd` Command

```
ldapadd -h myserver -p 12061 -D cn=fmwadmin -w mybiz1 -f managers.ldif -v
add labeleduri:
ldap://myserver.example.com:12061/cn=users,dc=us,dc=mybiz,dc=com??sub?(title=Ma
nager)
add description:
Dynamic Group of Managers
add cn:
Managers
add orclisvisible:
true
add objectclass:
orclDynamicGroup
orclGroup
top
groupOfUniqueNames
add displayname:
Managers
```

```

add owner:
cn=fmwadmin,cn=users,dc=us,dc=mybiz,dc=com
adding new entry
cn=managers,cn=portal.070720.104824.056918000,cn=groups,dc=us,dc=mybiz,dc=com
modify complete

```

29.9.2 Creating a Dynamic Group Using the Oracle Directory Services Manager

To create a dynamic group using ODSM:

1. Invoke Oracle Directory Services Manager (ODSM) and connect to the Oracle Internet Directory server.

Refer to section "Using Oracle Directory Services Manager" in the Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory for information on invoking and using the Oracle Directory Services Manager.
2. From the Go to list, select Data Browser.
3. Click the New Entry icon in the data browser.
4. Provide the DN and add the objectclasses `orclDynamicGroup` and `groupOfUniqueNames`.
5. On the Mandatory Properties tab, provide the CN attribute.
6. On the Optional Properties tab, provide the attributes for `labeleduri`.
7. Click OK to complete the definition of the dynamic group.

When you refresh the tree view you'll see the new group that you created. Note that group members will not be shown in ODSM.

29.10 Configuring the REST Service Identity Asserter

This section describes how to configure an identity asserter for the REST service. For the REST service, including REST service APIs, to be used with WebCenter Portal applications requires that an identity asserter be configured for it in the WebCenter domain identity store. The following sections show how to configure OPSS Trust Service instances and identity asserters for Oracle WebLogic Server.

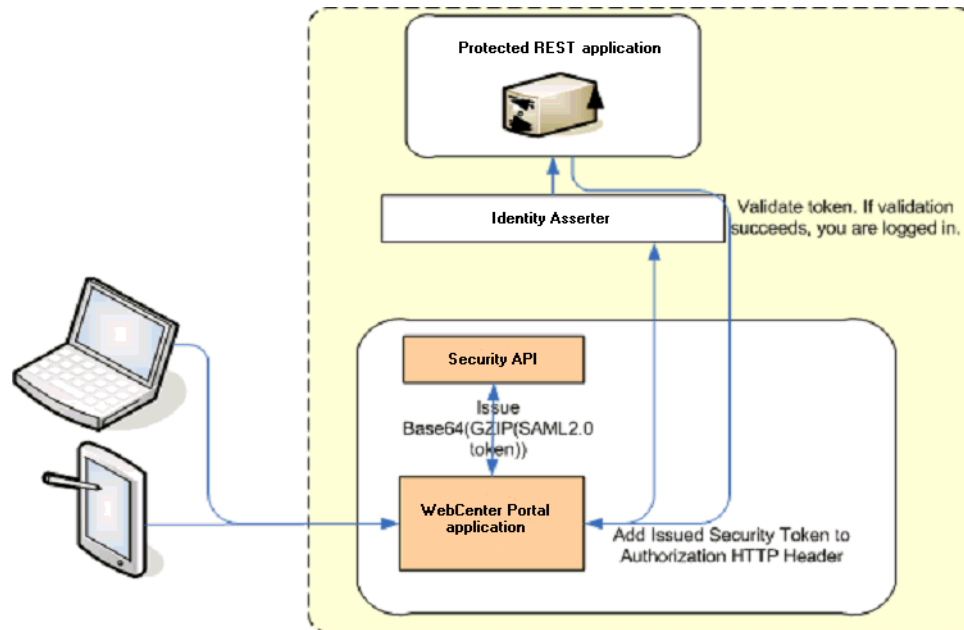
This section contains the following subsections:

- [Section 29.10.1, "Understanding the REST Service Instance and Identity Asserter"](#)
- [Section 29.10.2, "Setting up the Client Application"](#)
- [Section 29.10.3, "Configuring the WLS Trust Service Asserter"](#)

29.10.1 Understanding the REST Service Instance and Identity Asserter

Although WebCenter Portal applications, and other Oracle WebLogic applications, can use REST APIs to display information the way they need to, since such calls originate from the mid-tier, users will be prompted again to provide login credentials. To overcome this, we use perimeter authentication where the user identity is propagated in the HTTP header and asserted using the OPSS Trust Service Asserter.

In order to successfully propagate user identity from one application to another application, these applications must be using correctly configured Trust Service instances. [Figure 29-48](#) shows the different components involved in the identity propagation and assertion.

Figure 29–48 REST Identity Propagation and Assertion

The following depicts the sequence of events involved in REST identity propagation and assertion:

1. End clients (browsers, smart phone apps) connect to a WebCenter Portal application.
2. The application page queries data from REST APIs and builds its own UI on top and therefore needs to call the REST end point.
3. The WebCenter Portal application calls WebCenter Security API (`WCSecurityUtility.issueTrustServiceSecurityToken`) to issue the token used for securely propagating the user identity. The token is generated using the Trust Service Embedded Provider. Generated tokens are compressed to optimize token size and then BASE64-encoded to ensure that the token can be safely transported using an HTTP header.
4. The WebCenter Portal application takes the issued token and adds it against the "Authorization" security header. The client then dispatches the token as part of its call to the REST URI.
5. WebLogic Server checks if the identity asserter exists for the given token type.
6. The identity asserter parses and verifies that the token is using OPSS Trust Service APIs.
7. The asserter maps the username to a WLS username, a user Subject is established, and the call ends up on the REST application.
8. The REST application recognizes that the user is already an authenticated user and sends a response. The WebCenter Portal application uses the response and shows the page to the end user.

29.10.2 Setting up the Client Application

This section describes how to configure the client for a REST service identity asserter.

To configure the client for a REST service identity asserter:

- Using JDeveloper, create the client application.

The client application could be a JSE or a servlet application. The following example shows the skeleton of a sample client application.

```
// The authenticated username
// String user = "weblogic";
// URL of the target application
URL url = "http://host:port/destinationApp";
//-----

String b64EncodedToken = WCSecurityUtility.issueTrustServiceSecurityToken()

URLConnection connection = (URLConnection) url.openConnection();
connection.setRequestMethod("GET");
connection.setDoOutput(true);
connection.setReadTimeout(10000);
connection.setRequestProperty("Authorization", AUTH_TYPE_NAME + " " + b64tok);
connection.connect();
BufferedReader rd = new BufferedReader(new InputStreamReader(
    connection.getInputStream()));
StringBuilder sb = new StringBuilder();

String line = null;
while ((line = rd.readLine()) != null) {
    sb.append(line);
}
connection.disconnect();
System.out.println(sb.toString());
```

- Create and configure the keystore.

Create the keystore for the domain and then configure WebLogic Server for the identity asserter. The keystore is first provisioned for a client certificate and private key. The client certificate is then exported and imported into a trust key store.

- Create the keystore as shown in [Section 34.1.2.1, "Creating the WebCenter Portal Domain Keystore."](#)
 - Configure the keystore as shown in [Section 34.1.2.2, "Configuring the Keystore with WLST,"](#) or [Section 34.1.2.3, "Configuring the Keystore Using Fusion Middleware Control."](#)
- Edit the `jps-config.xml` configuration file.
 - Navigate to your `domain_home/config/fmwconfig` directory.
 - Open the `jps-config.xml` file in a text editor.
 - Modify the `trust.provider.embedded` propertySet node as below:

```
<propertySets>
  <propertySet name="trust.provider.embedded">
    ... existing entries
    <property value="orakey" name="trust.aliasName"/>
    <property value="orakey" name="trust.issuerName"/>
  </propertySet>
</propertySets>
```

Where:

`trust.aliasName` is the alias looked up by the identity asserter in the configured keystore for a certificate with which the asserter verifies the issued trust token.

`trust.issuerName` is the alias looked up by the token issuer to look up the private key with which the trust token is issued/signed.

4. If the client and REST applications are in different domains, repeat these steps for both domains.
5. Restart all servers.

29.10.3 Configuring the WLS Trust Service Asserter

This section describes how to configure the WebLogic Server Trust Service asserter.

To configure the WebLogic Server Trust Service asserter:

1. Log into the WebLogic Administration Console as an administrator.
2. Navigate to **Security Realms** -> **myrealm**.
3. Open the Providers tab, and then the Authentication subtab.

The Create a New Authentication Provider page displays.

4. Enter the **Name** of the new asserter (for example, `TrustServiceIdAsserter`).
5. Select `TrustServiceIdentityAsserter` as the asserter **Type**.

This asserter calls the Trust Service APIs to decode and validate the token from the incoming request, and pass the username to the WebLogic for establishing the asserted subject.

6. Click **OK** to save your changes.

Configuring the Policy and Credential Store

For production environments, you must reassociate your policy store with an external LDAP (either Oracle Internet Directory 11gR1 or 10.1.4.3), or a database. Note that when using an external LDAP-based store, the credential store and policy store must be configured to use the same LDAP server. The identity store can, however, use any of the other supported LDAP servers; it does not need to use the same LDAP server as the policy and credential stores.

Reassociating the policy and credential store with 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. Reassociating the policy and credential store with a database consists of setting up the schema and database connection in the RCU, and then migrating the policy and credential store to the database from the command line using WLST.

Caution: Before reassociating the policy store, be sure to back up the relevant configuration files:

- `jps-config.xml`
- `system-jazn-data.xml`

As a precaution, you should also back up the `boot.properties` file for the Administration Server for the domain.

This chapter contains the following sections:

- [Section 30.1, "Creating a root Node"](#)
- [Section 30.2, "Reassociating the Credential and Policy Store Using Fusion Middleware Control"](#)
- [Section 30.3, "Reassociating the Credential and Policy Store Using WLST"](#)
- [Section 30.4, "Reassociating the Policy and Credential Store with a Database"](#)
- [Section 30.5, "Managing Credentials"](#)
- [Section 30.6, "Managing Users and Application Roles"](#)
- [Section 30.7, "Configuring Self-Registration By Invitation in the Spaces Application"](#)
- [Section 30.8, "Setting the Policy Store Refresh Interval and Other Cache Settings"](#)

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."](#)

30.1 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_ORACLE_HOME/as_1/bin/ldapadd -h ldap_host_name -p ldap_port -D cn=orcladmin
-w password -v -f root.ldif
```

where:

- `OID_ORACLE_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.

30.2 Reassociating the Credential and Policy Store Using Fusion Middleware Control

Before reassociating the policy and credential store with Oracle Internet Directory, you must first have created the root node as described in [Section 30.1, "Creating a root Node."](#)

To reassociate the policy and credential store with the OID server:

1. Open Fusion Middleware Control and log in to 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.

When initially installed, Spaces and Enterprise Manager are already associated and deployed in the same domain.

3. From the WebLogic Domain menu, select **Security > Security Provider Configuration**.

The Security Provider Configuration page displays (see [Figure 30–1](#)).

Figure 30–1 Security Provider Configuration Page

wc_domain WebLogic Domain Logged in as weblogi
Page Refreshed Feb 13, 2012 11:31:41 AM PST

Security Provider Configuration

Use this page to configure global management domain policy and credential store providers, keystore and login modules used by Web Services Manager.

Security Stores

Current policy and credential store providers are shown below. To migrate the current policy and credential providers use the Change Store Type button.

[Change Store Type](#) [Edit](#)

Name	Store Type	Location
Policy Store		
Credential Store	LDAP	ldap://example.com:3060/cn=wc_domain,cn=root_webcenter
Keystore		

Identity Store Provider

To configure and manage Identity store provider in the WebLogic domain, use the [Oracle WebLogic Server Security Provider](#).

Configure parameters for User and Role APIs to interact with identity store. [Configure...](#)

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 Module
saml2.loginmodule	oracle.security.jps.internal.jaas.module.saml.JpsSAML2LoginModule	Required	SAML2 Login Module
krb5.loginmodule	com.sun.security.auth.module.Krb5LoginModule	Required	Kerberos Login Module
digest.authenticator.log	oracle.security.jps.internal.jaas.module.digest.DigestLoginModule	Required	Digest Authenticator
certificate.authenticator	oracle.security.jps.internal.jaas.module.x509.X509LoginModule	Required	X509 Certificate
wss.digest.loginmodule	oracle.security.jps.internal.jaas.module.digest.WSSDigestLoginModule	Required	WSS Digest Login Module
user.authentication.login	oracle.security.jps.internal.jaas.module.authentication.JpsUserAuthenticationModule	Required	User Authentication

Keystore

Single Sign-On Provider

Advanced Properties

4. On the Security Provider Configuration page, click **Change Store Type** to add the new Oracle Internet Directory provider (or select the store and click **Edit** if the store already exists and you want to change its parameters).

The Configure Security Stores page displays (see [Figure 30–2](#)).

Figure 30–2 *Configure Security Store Page*

Configure Security Stores OK Cmc

Specify server specific attributes to reassociate the policy, credential and key stores.

Store Type Oracle Internet Directory

LDAP Server Details

Provide valid credential to connect to LDAP server. Farm uses this credential to connect to LDAP server for authentication and authorization.

* Host

* Port

Use SSL to connect

* Connect DN Test LDAP Authentication

* Password

Root Node Details

Use this section to define provider specific configuration for this security store. To specify the 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.

* Root DN

Create New Domain

* Domain Name

Policy Store Properties

Specify policy store instance property configuration for getting maximum performance.

Enable Lazy Load Forced Refresh Time (secs)

Role Member Cache Size Refresh Polling Time (secs)

Permission Cache Size

Update Cache Incrementally for Management

Enable Store Refresh

Custom Properties

Property Name	Value
+ Add X Delete...	

Credential Store Properties

Custom Properties

Property Name	Value
+ Add X Delete...	

5. Select **Oracle Internet Directory** as the **Store Type**.
6. Under **LDAP Server Details**, enter the **Host** name and **LDAP Port** for Oracle Internet Directory.
7. Set the **Connect DN** field to `cn=orcladmin`, and enter the associated password in the **Password** field.
8. Under **Root Node Details**, set the **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.

30.3 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 30.1, "Creating a root Node."](#)

1. Start WLST as described in [Section 1.13.3.1, "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. Specify `OID` for Oracle Internet 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")
```

30.4 Reassociating the Policy and Credential Store with a Database

As well as using an LDAP server, such as OID, for your policy and credential store, you can also reassociate the policy and credential store with an Oracle database. Prior to reassociating the policy and credential store with a database, you should have:

- Installed the RCU and the OPSS schema
- Installed an Oracle database (Oracle RDBMS version 10.2.0.4+, 11.1.0.7+, or 11.2.0.1+)
- Installed WebLogic Server
- Created a domain

For instructions on how to create a new domain, see "Creating a New Domain" in the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Portal*.

- Created a data source

For instructions on how to create a data source, see "Creating a JDBC Data Source" in the *Oracle Fusion Middleware Configuring and Managing JDBC Data Sources for Oracle WebLogic Server*.

- Backed up your `<DOMAIN>/config/fmwconfig/jps-config.xml` file.

Follow the steps below to configure a database as your policy and credential store:

1. Associate the schema and database connection. For information about how to associate the schema and database connection, see [Section 7.1.5, "Creating and Registering the Metadata Service Repository."](#)
2. Back up the `jps-config.xml` and `bootstrap/cwallet.sso` files (both are in the `domain_home/config/fmwconfig` folder).
3. Migrate the policy and credential store to the database using the following WLST command:

```
reassociateSecurityStore(domain="your_domain",
datasourcename="your_data_source", servertime="DB_ORACLE",
jpsroot="cn=jpsTestNode")
```

Where `datasourcename` is the JNDI name for the OPSS data source you just created. Note also that `jpsroot` is the parameter through which the policy store gets striped, and the value of this parameter should be unique to the policy store. For more information about using the `reassociateSecurityStore` command, see "reassociateSecurityStore" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

30.5 Managing Credentials

Administrators can manage credentials for the WebCenter Portal domain credential store using Fusion Middleware Control and WLST commands. For more information, see "Managing Credentials" in the *Oracle Fusion Middleware Application Security Guide*.

30.6 Managing Users and Application Roles

This section describes how you can use Fusion Middleware Control, WLST, and the runtime administration pages in Spaces and Framework applications to manage users and application roles.

This section contains the following subsections:

- [Section 30.6.1, "Granting the Spaces Administrator Role"](#)
- [Section 30.6.2, "Granting Application Roles"](#)
- [Section 30.6.3, "Using the Runtime Administration Pages"](#)

30.6.1 Granting the Spaces Administrator Role

Spaces only recognizes users in the identity store that is mapped by the first authenticator. Since the 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 Spaces, you must also create a user in that LDAP and grant that user the Spaces Administrator role.

You can grant a user the Spaces Administrator role using Fusion Middleware Control or WLST as shown below in the sections on:

- [Section 30.6.1.1, "Granting the Spaces Administrator Role Using Fusion Middleware Control"](#)
- [Section 30.6.1.2, "Granting the Spaces Administrator Role Using WLST"](#)

For more information, see "Granting the Administrator Role to a Non-Default User" in the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Portal*.

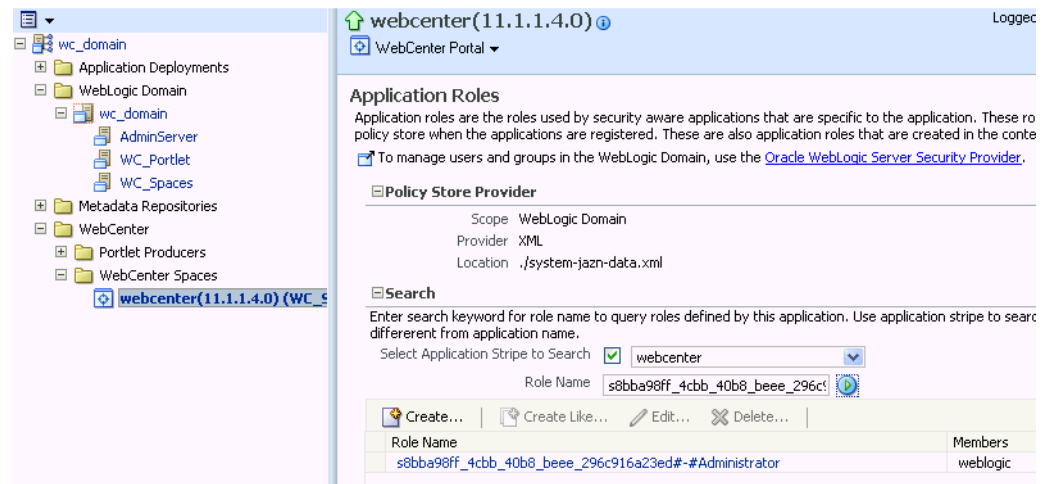
30.6.1.1 Granting the Spaces Administrator Role Using Fusion Middleware Control

This section describes how to grant the Spaces administrator role to a user account other than the default "weblogic" account.

To grant the Spaces Administrator role using Fusion Middleware Control:

1. Log into Fusion Middleware Control and navigate to the Spaces home page.
See [Section 6.2, "Navigating to the Home Page for the Spaces Application."](#)
2. From the WebCenter Portal menu, select **Security -> Application Roles**.
The Application Roles page displays (see [Figure 30–3](#)).

Figure 30–3 Application Roles Page



3. Search for the Spaces Administrator role:
 - a. Select **Select Application Stripe to Search**.
 - b. Select `webcenter`.
 - c. In the **Role Name** field, enter the following internal identifier for the Administrator role, and then click the **Search** (arrow) icon:

```
s8bba98ff_4cbb_40b8_beee_296c916a23ed#-#Administrator
```

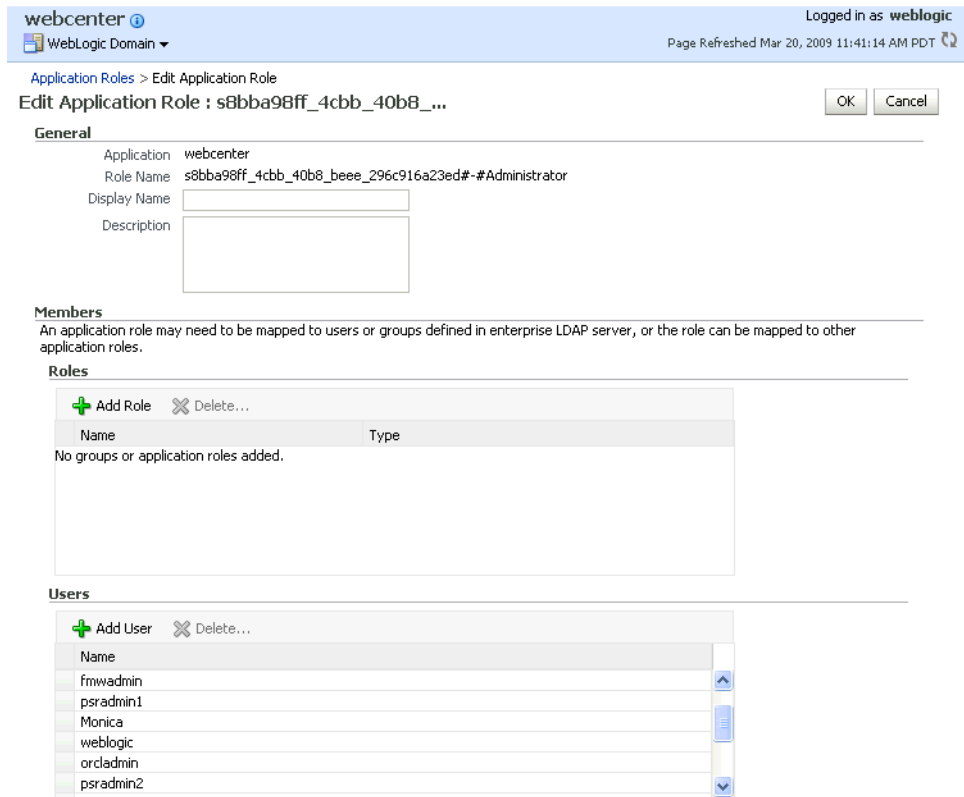
The search should return

```
s8bba98ff_4cbb_40b8_beee_296c916a23ed#-#Administrator, which is the administrator role identifier.
```

4. Click the administrator role identifier in the Role Name column.

The Edit Application Role page displays (see [Figure 30–4](#)).

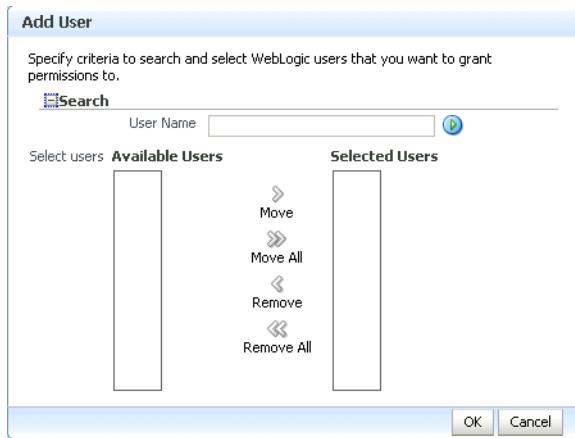
Figure 30–4 Edit Application Role Page



5. Click **Add User**.

The Add User pop-up displays (see [Figure 30–5](#)).

Figure 30–5 Add User Pop-up



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. To remove the weblogic role, on the Edit Application Role page under **Users**, click **weblogic** and the click **Delete**.

- Restart the `WC_Spaces` managed server.

When you login to Spaces, the Administration link should appear and you should be able to perform all administrator operations.

30.6.1.2 Granting the Spaces Administrator Role Using WLST

To grant the Spaces Administrator role to another user using WLST:

- Start WLST as described in [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)
- Connect to the 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).
- Grant the 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.

- To test the new account, log into Spaces using the new account name. The Administration link should appear, and you should be able to perform all administrator operations.
- After granting the Spaces Administrator role to new accounts, remove this role from accounts that no longer need or require it using the WLST `revokeAppRole` command. For example, if 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")
```

30.6.2 Granting Application Roles

This section describes how to add users to application roles using Fusion Middleware Control and WLST commands.

This section contains the following subsections:

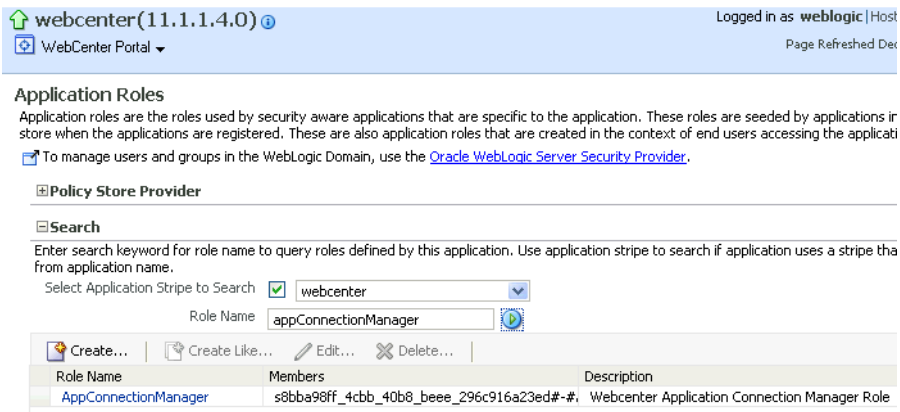
- [Section 30.6.2.1, "Granting Application Roles Using Fusion Middleware Control"](#)
- [Section 30.6.2.2, "Granting Application Roles Using WLST"](#)

30.6.2.1 Granting Application Roles Using Fusion Middleware Control

This section describes how to grant an application role to users using Fusion Middleware Control.

1. Log in to Fusion Middleware Control and navigate to the home page for Spaces or your Framework application. For more information, see:
 - [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#)
 - [Section 6.3, "Navigating to the Home Page for Framework Applications"](#)
2. From the WebCenter Portal menu, select **Security -> Application Roles**.
The Application Roles page displays (see [Figure 30–6](#)).

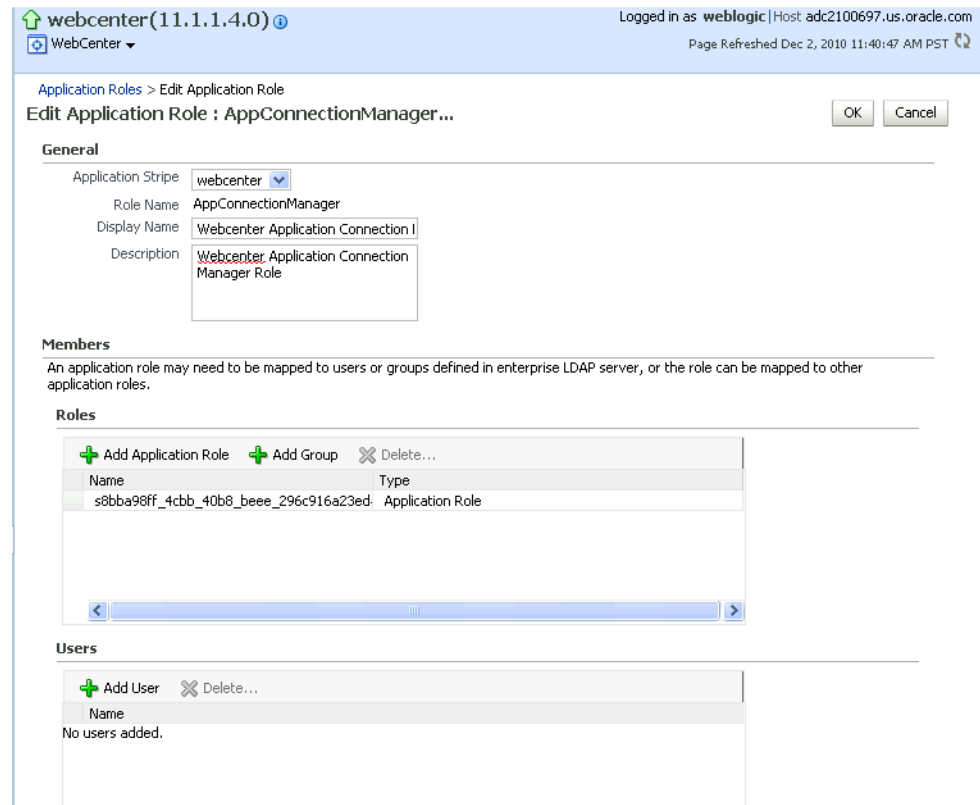
Figure 30–6 Application Roles Page



3. Search for the Spaces or Framework application role:
 - a. Select **Select Application Stripe to Search**.
 - b. Select the application stripe (webcenter for Spaces).
 - c. In the **Role Name** field, enter the name of the role you are looking for (for example, appConnectionManager), and then click the **Search** (arrow) icon:

If you are not sure of the name, enter a partial search term or leave the field blank to display all the application roles.
4. Click the role identifier in the Role Name column.
The Edit Application Role page displays (see [Figure 30–7](#)).

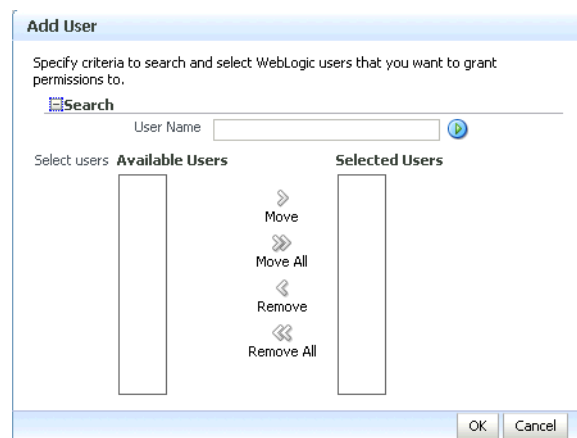
Figure 30–7 Edit Application Role Page



5. Click **Add User**.

The Add User pop-up displays (see [Figure 30–8](#)).

Figure 30–8 Add User Pop-up



6. Use the Search function to search for the user to assign the application 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. Restart the managed server on which Spaces or the Framework application is deployed (for Spaces this is always WC_Spaces).

30.6.2.2 Granting Application Roles Using WLST

Use the `grantAppRole` command to grant an application role to a user. For syntax and usage information, see "grantAppRole" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

30.6.3 Using the Runtime Administration Pages

Spaces provides a *Security tab* from which an administrator can define application roles and grant application roles to users defined in the identity store. For information about managing users and application roles in Spaces, see "Managing Users and Roles for WebCenter Portal: Spaces" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

Caution: The "Allow Password Change" property, which specifies whether users can change their passwords within Spaces, should be carefully controlled for corporate identity stores. Spaces administrators can set this property from the Profile Management Settings page in Spaces. For more information, see "Configuring Profiles" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

Framework applications can provide a similar Security tab for application administrators. For details, see [Section 36.4, "Managing Application Members and Roles."](#) For more information about role-mapping for ADF-security based Framework 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*.

30.7 Configuring Self-Registration By Invitation in the Spaces Application

Spaces supports self-registration by invitation, as described in "Enabling Self-Registration By Invitation-Only" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*. The self-registration 'by-invitation' feature requires that the WebCenter Portal domain credential store contain the following password credentials:

- `map name = o.webcenter.security.selfreg`
- `key= o.webcenter.security.selfreg.hmackey`
- `user name = o.webcenter.security.selfreg.hmackey`

To enable 'self-registration by invitation' in Spaces, use Fusion Middleware Control or the WLST command `createCred` to create the password credentials detailed above. For example:

```
createCred(map="o.webcenter.security.selfreg",  
key="o.webcenter.security.selfreg.hmackey", type="PC",  
user="o.webcenter.security.selfreg.hmackey", password="<password>", url="<url>",  
port="<port>", [desc="<description>"])
```

For more information, see "Managing Credentials" in the *Oracle Fusion Middleware Application Security Guide*.

30.8 Setting the Policy Store Refresh Interval and Other Cache Settings

This section provides recommended cache settings that should be configured after installation. Although settings for cache sizes and maximum group hierarchies should be based on your specific environment, the following sections provide recommendations that you can use as a starting point. For a complete list of tuning parameters and recommended values for WebCenter Portal, see "Oracle WebCenter Portal Performance Tuning" in the Oracle Fusion Middleware Performance and Tuning Guide.

This section includes the following subsections:

- [Section 30.8.1, "Setting the Policy Store Refresh Interval"](#)
- [Section 30.8.2, "Setting the Connection Pool Cache"](#)
- [Section 30.8.3, "Setting User Cache Settings"](#)
- [Section 30.8.4, "Setting Group Cache Settings"](#)

30.8.1 Setting the Policy Store Refresh Interval

The authorization policies used by WebCenter Portal use an in-memory cache with a default policy refresh time of 10 minutes. When a group space is created in a multi-node high availability environment, and you need a node failure to replicate the policy data more quickly, you can shorten the policy store refresh interval by modifying the domain-level `jps-config.xml` file, and adding the following entry:

```
oracle.security.jps.ldap.policystore.refresh.interval=<time_in_milli_seconds>
```

This should be added to the PDP service node:

```
<serviceInstance provider="pdp.service.provider" name="pdp.service">
```

Note that the policy refresh interval should not be set to too small a value as the frequency at which the server cached policy is refreshed may impact performance.

After modifying the `jps-config.xml` file, restart all servers in the domain. For more information, see "Caching and Refreshing the Cache" in the Oracle Fusion Middleware Application Security Guide.

30.8.2 Setting the Connection Pool Cache

This section describes the recommended settings for the connection pool cache.

To set the connection pool cache:

1. Log into the WLS Administration Console.
2. Select **Security Realms** > *[realm]* > **Providers** > *[provider]* > **Configuration** > **Provider Specific**.
3. Set the connection pool cache parameters to the following recommended values:
 - **Connection Pool Size** = max connection users
 - **Connect Timeout** = 30
 - **Connection Retry Limit** = 1
 - **Results Time Limit** = 1000
 - **Keep Alive Enable** = true
4. Save your changes and restart all servers in the domain.

30.8.3 Setting User Cache Settings

This section describes the recommended settings for user cache settings.

To set user cache settings:

1. Log into the WLS Administration Console.
2. Select **Security Realms** > *[realm]* > **Providers** > *[provider]* > **Configuration** > **Provider Specific**.
3. Set the user cache parameters to the following recommended values:
 - **Cache Enabled** = `true`
 - **Cache Size** = 3200
 - **Cache TTL** = `session timeout`
 - **Results Time Limit** = 1000
 - **Keep Alive Enable** = `true`
4. Save your changes and restart all servers in the domain.

30.8.4 Setting Group Cache Settings

This section describes the recommended settings for group cache settings.

To set group cache settings:

1. Log into the WLS Administration Console.
2. Select **Security Realms** > *[realm]* > **Providers** > *[provider]* > **Performance**.
3. Set the group cache parameters to the following recommended values:
 - **Enable Group Membership Lookup Hierarchy Caching** = `true`
 - **Cache Size** = 3200
 - **Max Group Hierarchies in Cache** = 1024
 - **Group Hierarchy Cache TTL** = `session timeout`
 - **Keep Alive Enable** = `true`
4. Save your changes and restart all servers in the domain.

Configuring Single Sign-on

This chapter describes the available single sign-on (SSO) solutions for your WebCenter Portal application to use, and how each is configured.

This chapter includes the following sections:

- [Section 31.1, "Introduction to Single Sign-on"](#)
- [Section 31.2, "Configuring Oracle Access Manager \(OAM\)"](#)
- [Section 31.3, "Configuring Oracle Single Sign-On \(OSSO\)"](#)
- [Section 31.4, "Configuring SAML-based Single Sign-on"](#)
- [Section 31.5, "Configuring SSO for Microsoft Clients"](#)
- [Section 31.6, "Configuring SSO with Virtual Hosts"](#)

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."](#)

31.1 Introduction to Single Sign-on

Single sign-on can be implemented for WebCenter Portal applications (Spaces and Framework applications) using several solutions. This section describes their benefits and recommended application.

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 Spaces and Framework applications. OAM (in particular, OAM 11g) is the recommended single sign-on solution for Oracle WebCenter Portal 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 Portal 11g can also be configured to use OSSO for single sign-on.

For non-production, development environments 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 Spaces and its associated Web applications like Discussions, and Worklist, you can configure a

SAML-based SSO solution. If you need to provide single sign-on for other enterprise applications as well, 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.

31.2 Configuring Oracle Access Manager (OAM)

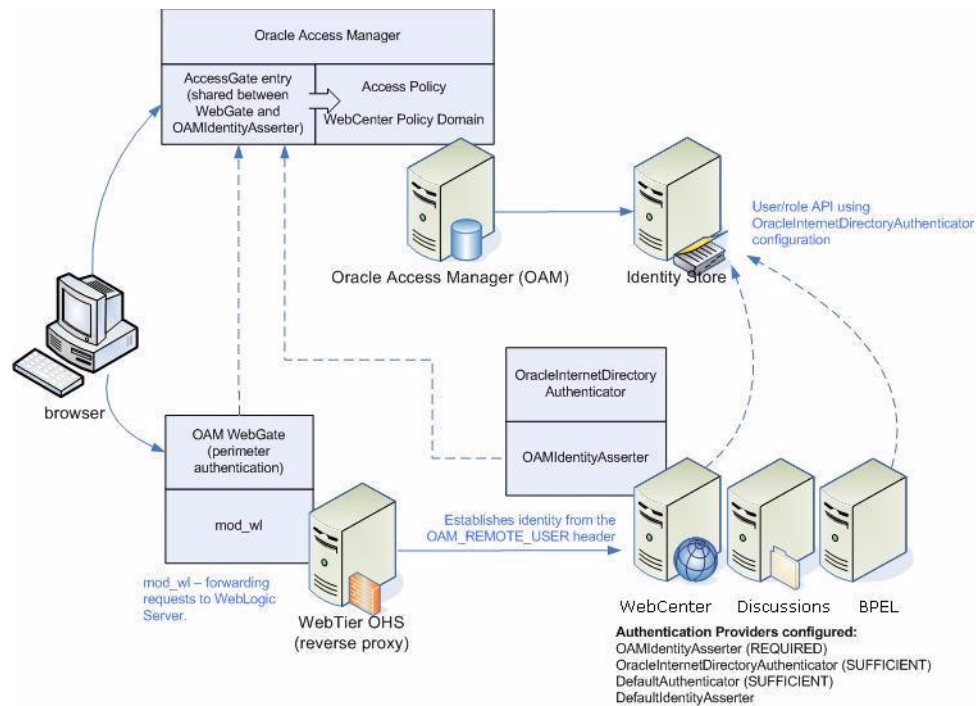
Oracle Access Manager (OAM) provides flexible and extensible authentication and authorization, and provides audit services. This section describes how to configure Spaces and Framework applications for OAM single sign-on authentication, including how to configure the WebLogic server side and the WebCenter Portal application as the partner application participating in SSO. Note that for Framework applications some additional configurations are required, as described in [Section 32.4, "Configuring Framework and Portlet Producer Applications for OAM."](#)

The installation and configuration steps for OAM 11g and 10g are presented in the following subsections:

- [Section 31.2.1, "OAM Components and Topology"](#)
- [Section 31.2.2, "Roadmap to Configuring OAM"](#)
- [Section 31.2.3, "Installing and Configuring OAM"](#)
- [Section 31.2.4, "Configuring the WebLogic Domain for OAM"](#)
- [Section 31.2.5, "Installing and Configuring the Oracle HTTP Server"](#)
- [Section 31.2.6, "Additional Single Sign-on Configurations"](#)
- [Section 31.2.7, "Testing Your OAM Installation"](#)

31.2.1 OAM Components and Topology

[Figure 31–1](#) shows the components and topology required to set up single sign-on with Oracle Access Manager for a WebCenter Portal application.

Figure 31–1 OAM Single Sign-On Components and Topology

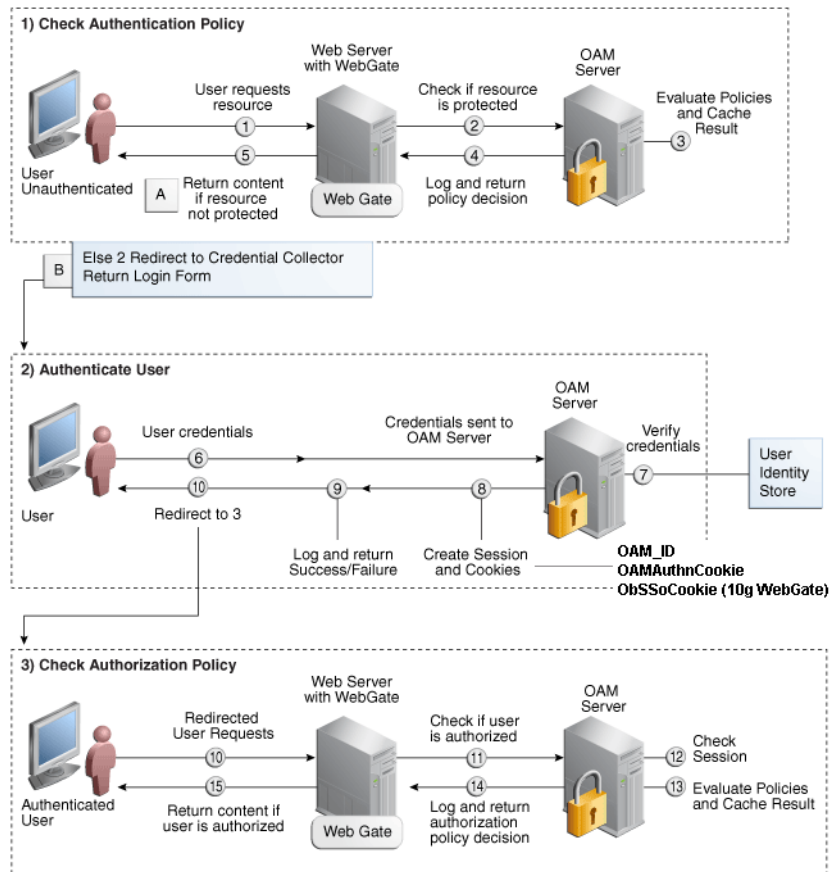
OAM consists of the following components:

- **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.

OAM Single Sign-on Process Flow

Figure 31–2 shows the single sign-on process flow for OAM.

Figure 31–2 OAM Single Sign-on Process Flow



SSO Log-in Processing with OAM Agents

1. The user requests a resource.
2. The WebGate forwards the request to OAM for policy evaluation.
3. OAM:
 - Checks for the existence of an SSO cookie.
 - Checks policies to determine if the resource protected and if so, how?
4. The OAM server logs and returns decisions.
5. WebGate responds as follows:
 - Unprotected resource: resource is served to the user.
 - Protected resource:
 - Request is redirected to the credential collector
 - The login form is served based on the authentication policy
 - Authentication processing begins
6. User sends credentials.
7. OAM verifies credentials.
8. OAM starts the session and creates the following host-based cookies:

- One per partner: `OAMAuthnCookie` set by 11g WebGates (`ObSSOCookie` set by 10g WebGate) using the authentication token received from the OAM server after successful authentication.
Note: A valid cookie is required for a session.
 - One for OAM Server: `OAM_ID`
9. OAM logs Success or Failure.
 10. OAM Credential collector redirects to WebGate and authorization processing begins.
 11. WebGate prompts OAM to look up policies, compare them to the user's identity, and determine the user's level of authorization.
 12. OAM logs policy decision and checks the session cookie.
 13. OAM Server evaluates authorization policies and cache the result.
 14. OAM Server logs and returns decisions
 15. WebGate responds as follows:
 - If the authorization policy allows access, the request get redirected to `mod_wl` which in turn redirects the request to the WLS server where the Spaces application is running, and from where desired content or applications are served to the user, as shown below:
WebGate -> mod_wl -> Spaces [, Discussion, .. etc] --> Content is server to the authenticated user
 - If the authorization policy denies access, the user is redirected to another URL determined by the administrator.

31.2.2 Roadmap to Configuring OAM

The flow chart (Figure 31-3) and table (Table 31-1) in this section provide an overview of the prerequisites and tasks required to configure single sign-on for WebCenter Portal using OAM.

Figure 31–3 Configuring Single Sign-on for WebCenter Portal Using OAM

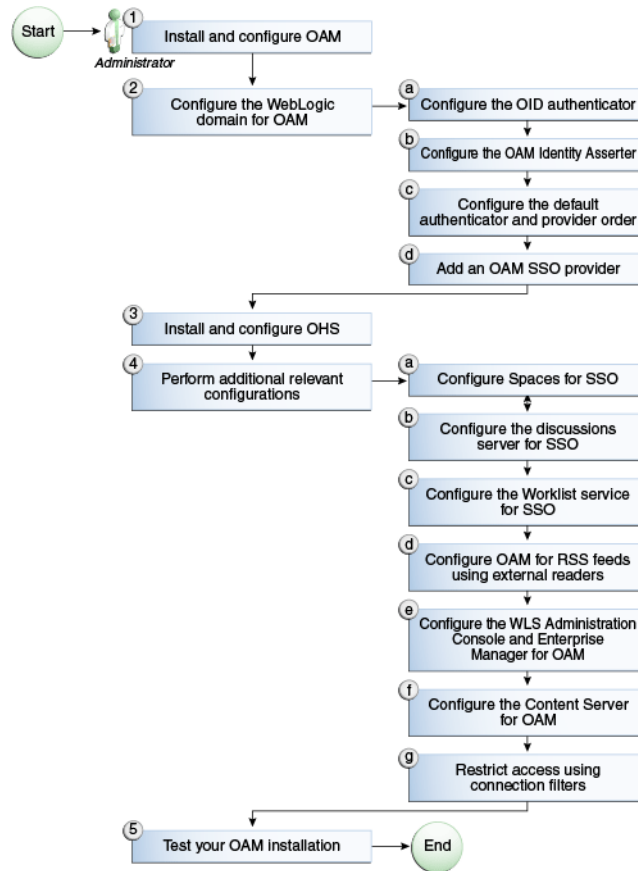


Table 31–1 shows the tasks and sub-tasks for configuring single sign-on for WebCenter Portal using OAM.

Table 31–1 Configuring Single Sign-on for WebCenter Portal Using OAM

Actor	Task	Sub-task	Notes
Administrator	1. Install and Configure OAM		Install and configure OAM 10g or 11g.
	2. Configure the WebLogic domain for OAM	2.a Configure the OID authenticator 2.b Configure the OAM identity asserter 2.c Configure the default authenticator and provider order 2.d Add an OAM SSO provider	
	3. Install and configure OHS		
	4. Perform additional configurations as required	4.a Configure Spaces for SSO 4.b Configure the discussions server for SSO	

Table 31–1 (Cont.) Configuring Single Sign-on for WebCenter Portal Using OAM

Actor	Task	Sub-task	Notes
		4.c Configure the Worklist service for SSO	
		4.d Configure OAM for RSS feeds using external readers	
		4.e Configure the WLS Administration Console and Enterprise Manager for OAM 11g or OAM 10g	
		4.f Configure Content Server for OAM	
		4.g Restrict access using connection filters	
	5. Test your OAM installation		

31.2.3 Installing and Configuring OAM

This section describes how to install and configure either OAM 11g or OAM 10g, the recommended single sign-on solutions for WebCenter Portal installations.

Note: Installing OAM should be performed only after you've installed Oracle WebCenter Portal (described in the *Oracle Fusion Middleware Installation Guide for Oracle WebCenter Portal*) and any other components required for your environment. You should also have configured and tested any required connections.

This section includes the following subsections:

- [Section 31.2.3.1, "Installing and Configuring OAM 11g"](#)
- [Section 31.2.3.2, "Installing and Configuring OAM 10g"](#)

31.2.3.1 Installing and Configuring OAM 11g

This section describes how to install and configure OAM 11g, and includes the following subsections:

- [Section 31.2.3.1.1, "Installing and Configuring OAM 11g"](#)
- [Section 31.2.3.1.2, "Installing and Configuring the Oracle HTTP Server"](#)
- [Section 31.2.3.1.3, "Installing the WebGate on the WebTier"](#)
- [Section 31.2.3.1.4, "Registering the WebGate Agent"](#)

31.2.3.1.1 Installing and Configuring OAM 11g

Install Oracle Access Manager (OAM) as described in "Installing the Oracle Identity Management 11g Software" in the Oracle Fusion Middleware Installation Guide for Oracle Identity Management. Ideally, OAM and all the applications that participate in single sign-on should share the same identity store. By default, OAM uses the embedded LDAP identity store.

To configure OAM to use an external identity store, such as OID, see "Registering a New Identity Store" in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*. This section has pointers to setting the external identity store configured as the default or system store and configuring one or more authentication modules to point to this store. By default, the WebCenter policy configured in OAM uses the default authentication scheme (typically, the form-based

authentication scheme `LDAPScheme`) specified in OAM. If you intend to use the default scheme, the authentication module used by the scheme must point to the same identity store as your WebCenter installation. Optionally, you can choose to configure a different authentication scheme rather than the default, in which case you must also ensure that it points to the identity store used by WebCenter. Continue by configuring Oracle Access Manager in a WebLogic administration domain as described in "Configuring Oracle Access Manager (OAM)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

31.2.3.1.2 Installing and Configuring the Oracle HTTP Server

If you don't already have Oracle HTTP Server (OHS) installed, install OHS (11.1.1.4.0) as described in [Section 31.2.5, "Installing and Configuring the Oracle HTTP Server."](#)

If you do have an existing installation, you will need to apply a patch to bring it up to OHS (11.1.1.4.0) as described in "Applying the Latest Oracle Fusion Middleware Patch Set" in the Oracle Fusion Middleware Patching Guide.

After installing or patching OHS, continue by installing the WebGate as described in [Section 31.2.3.1.3, "Installing the WebGate on the WebTier."](#)

31.2.3.1.3 Installing the WebGate on the WebTier

This section describes how to install and configure the OHS WebGate.

Note: Ensure that your Oracle HTTP server is down while installing OHS WebGate, and restart it only after you register the WebGate agent as described in [Section 31.2.3.1.4, "Registering the WebGate Agent."](#)

1. For Linux and Solaris operating systems, download and install the third-party GCC libraries to the same location where OHS is installed as described in "Installing Third-Party GCC Libraries (Linux and Solaris Operating Systems Only)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.
2. Install the WebGate as described in the section on "Installing Oracle HTTP Server 11g WebGate for Oracle Access Manager" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*. Use the same middleware home that was specified during OHS install. Note that during the installation you will need to point to the directory containing the GCC libraries downloaded in the previous step.
3. After installing Oracle HTTP Server 11g WebGate for Oracle Access Manager, move to the following directory under your Oracle Home for Webgate:

For Unix operating systems:

```
<Webgate_Home>/webgate/ohs/tools/deployWebGate
```

For Windows operating systems:

```
<Webgate_Home>\webgate\ohs\tools\deployWebGate
```

4. From the command line, run the following command to copy the required bits of the agent from the `Webgate_Home` directory to the WebGate instance location:

For Unix operating systems:

```
./deployWebGateInstance.sh -w <Webgate_Instance_Directory> -oh
```

<Webgate_Oracle_Home>

For Windows operating systems:

```
deployWebGateInstance.bat -w <Webgate_Instance_Directory> -oh
<Webgate_Oracle_Home>
```

Where <Webgate_Oracle_Home> is the directory where you have installed Oracle HTTP Server WebGate and defined it as the Oracle Home for WebGate, as in the following example:

```
<MW_HOME>/Oracle_OAMWebGate1
```

The <Webgate_Instance_Directory> is the location of the Webgate Instance Home (which should be the same as the Instance Home of Oracle HTTP Server), as in the following example:

```
<MW_HOME>/Oracle_WT1/instances/instance1/config/OHS/ohs1
```

Note that an Instance Home for Oracle HTTP Server is created after you configure the Oracle HTTP Server. This configuration should be performed after installing or patching to Oracle HTTP Server 11.1.1.4.0.

5. Run the following command to ensure that the LD_LIBRARY_PATH variable contains <Oracle_Home_for_Oracle_HTTP_Server>/lib:

For Unix operating systems (depending on the shell):

```
export
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:<Oracle_Home_for_Oracle_HTTP_Server>/lib
```

For Windows operating systems:

Add the <Webgate_Installation_Directory>\webgate\ohs\lib and <Oracle_Home_for_Oracle_HTTP_Server>\bin locations to the PATH environment variable. Add a semicolon (;) followed by this path at the end of the entry for the PATH environment variable.

6. From your current working directory, move up one level:

For Unix operating systems, move to:

```
<Webgate_Home>/webgate/ohs/tools/setup/InstallTools
```

For Windows operating systems, move to:

```
<Webgate_Home>\webgate\ohs\tools\EditHttpConf
```

7. From the command line, run the following command to copy the apache_webgate.template from the Webgate_Home directory to the WebGate Instance location (renaming it to webgate.conf) and update the httpd.conf file to add one line to include the name of webgate.conf file:

For Unix operating systems:

```
./EditHttpConf -w <Webgate_Instance_Directory> [-oh <Webgate_Oracle_Home>] [-o
<output_file>]
```

For Windows operating systems:

```
EditHttpConf.exe -w <Webgate_Instance_Directory> [-oh <Webgate_Oracle_Home>]
[-o <output_file>]
```

Note: The `-oh <WebGate_Oracle_Home>` and `-o <output_file>` parameters are optional.

Where `<Webgate_Oracle_Home>` is the directory where you have installed Oracle HTTP Server WebGate and defined it as the Oracle Home for WebGate, as in the following example:

```
<MW_HOME>/Oracle_OAMWebGate1
```

The `<Webgate_Instance_Directory>` is the location of the Web Gate instance home (which should be the same as the instance home of OHS), as in the following example:

```
<MW_HOME>/Oracle_WT1/instances/instance1/config/OHS/ohs1
```

31.2.3.1.4 Registering the WebGate Agent

After installing the WebGate on the WebTier, you also need to register the WebGate agent. The steps below will automatically create a protected policy that uses the default Authentication Scheme that is configured in your OAM installation (typically, the form-based authentication scheme `LDAPScheme`). If you want to customize WebCenter Portal's single sign-on login page, or want WebCenter Portal resources to be protected by some other authentication scheme, then change it using the OAM Console (see "Managing Authentication Schemes" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service* for more information).

Note: If you are using WebCenter Portal in conjunction with other applications in your environment, and you require single sign-on for these applications, you must ensure that the authentication schemes used by these applications are either the same or at least at the same level and point to the same identity store.

For more information about registering the WebGate agent, see also "Getting Started with a New Oracle HTTP Server 11g Webgate Agent for Oracle Access Manager" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

Follow the steps below to register the WebGate agent on the machine where OAM is installed using the `oamreg` tool in inband mode:

1. Change directories to `<RREG_Home>/input`.
2. Copy over `$WEBCENTER_HOME/webcenter/scripts/webcenter.oam.conf` from the WebCenter Portal installation here.
3. Copy over `$SOA_HOME/soa/prov/soa.oam.conf` and `$WC_CONTENT_ORACLE_HOME/common/security/oam.conf` from the SOA and Content Server installations respectively.
4. Create a new file named `WebCenterOAM11gRequest.xml` to serve as a parameter file to the `oamreg` tool.

In the example below, replace the contents within `$$webtier..$$` with your WebTier host and port IDs, and `$$oam..$$` with the OAM host and administration server port.

```
<?xml version="1.0" encoding="UTF-8"?>
```

```

<!--
  Copyright (c) 2009, 2010, Oracle and/or its affiliates. All rights reserved.

  NAME: OAM11GRequest_short.xml - Template for OAM 11G Agent Registration
  Request file
  (Shorter version - Only mandatory values - Default values will be used for all
  other fields)
  DESCRIPTION: Modify with specific values and pass file as input to the tool.
-->
<OAM11GRegRequest>
  <serverAddress>http://$$oamhost$$:$$oamadminserverport$$</serverAddress>
  <hostIdentifier>$$webtierhost$$_webcenter</hostIdentifier>
  <agentName>$$webtierhost$$_webcenter</agentName>
  <logoutUrls>
    <url>/oamssso/logout.html</url>
  </logoutUrls>
</OAM11GRegRequest>

```

5. Change directories to `<RREG_Home>`.

6. Run the following command:

```
<RREG_Home>/bin/oamreg.sh inband input/WebCenterOAM11gRequest.xml
```

- When prompted for agent credentials enter your OAM administrator credentials.
- Enter your WebGate password.
- Enter `yes` when asked whether you want to import a URIs file. Specify the full path to the `<RREG_HOME>/input/webcenter.oam.conf` file you copied there earlier.

You should see output like that below indicating that registration has been successful:

```

-----
Request summary:
OAM11G Agent Name:example_webcenter
URL String:example_webcenter
Registering in Mode:inband
Your registration request is being sent to the Admin server at:
http://example.com:7001
-----

```

Inband registration process completed successfully! Output artifacts are created in the output folder.

7. Copy the generated files and artifacts (`ObAccessClient.xml` and `cwallet.sso`) from `<RREG_Home>/output/$$webtierhost$$_webcenter` to your WebGate instance configuration directory (`<Webgate_Instance_Directory>/webgate/config`). Note that `<Webgate_Instance_Directory>` should match the instance home of OHS, as in the following example:

```
<MW_HOME>/Oracle_WT1/instances/instance1/config/OHS/ohs1/webgate/config
```

8. Change directories to `<RREG_Home>/input`.

9. If you have SOA or WebCenter Content Server installed

- a. Create a policy update file called `WebCenterOAM11gPolicyUpdate.xml` as shown in the example below, replacing the contents within `$$webtier..$$`

with your WebTier host and port IDs, and `$$oam...$$` with the OAM host and administration server port as you did earlier:

```
<?xml version="1.0" encoding="UTF-8"?>

<!--
  Copyright (c) 2009, 2011, Oracle and/or its affiliates. All rights
  reserved.

  NAME: UpdatePolicyRequest.xml - Template for updating application domain
  and/or policies without changes to any agent profile
  DESCRIPTION: Modify with specific values and pass file as input to the
  tool
-->
<PolicyRegRequest>

  <serverAddress>http://$$oamhost$$:$$oamadminserverport$$</serverAddress>
    <hostIdentifier>$$webtierhost$$_webcenter</hostIdentifier>

  <applicationDomainName>$$webtierhost$$_webcenter</applicationDomainName>

</PolicyRegRequest>
```

b. Run the following command:

```
<RREG_Home>/bin/oamreg.sh policyUpdate
input/WebCenterOAM11gPolicyUpdate.xml
```

Enter your OAM credentials when prompted. Enter *yes* when asked whether you want to import a URIs file, and specify

```
<RREG_HOME>/input/soa.oam.conf.
```

Your policy will be updated with SOA resources.

c. Run the `policyUpdate` command again, this time specifying `<RREG_HOME>/input/oam.conf` to update the policy with Content Server resources. Your policy now contains WebCenter Portal, SOA and Content Server artifacts.

10. From the OAM Console, you should now be able to see the following artifacts:

- 11g WebGate agent named `$$webtierhost$$_webcenter`
- 11g host identifier by the same name
- an application domain with the same name containing authentication and authorization policies which in turn contain protected and public policies

11. Go to **Application Domain** > `$$webtierhost$$_webcenter` > **Authentication Policies**. You should be able to see the following policies:

- Exclusion Scheme
- Protected Resource Policy
- Public Resource Policy
- WebCenter REST Policy

12. Open the WebCenter REST Policy and make sure that the Authentication Scheme is set to `BasicSessionlessScheme` or `BasicScheme`.

13. Open the Resources tab and search for resources with their Authentication Policy set to `Exclusion Scheme`. You should see the following resources:

- /rsscrawl*
- /rsscrawl/.../*
- /sesUserAuth*
- /sesUserAuth/.../*
- /services-producer/portlets*
- /services-producer/portlets/.../*
- /wsrp-tools/portlets
- /wsrp-tools/portlets/.../*

14. Select the /rsscrawl* resource in the search results and click Edit.

15. Change the Protection Level from Protected to Excluded and click **Apply**. Note that the resource's authentication policy and authorization policy is removed.

16. Close the Resources tab and repeat the steps for the remaining Exclusion Scheme resources.

When you now search for resources with their Authentication Policy set to Exclusion Scheme you should see no results.

17. Restart OHS.

18. After installing and configuring the WebTier and associated components, continue by configuring the Policy Manager as described in [Section 31.2.4, "Configuring the WebLogic Domain for OAM,"](#) and performing any additional service and component configurations that apply as described in [Section 31.2.6, "Additional Single Sign-on Configurations."](#)

31.2.3.2 Installing and Configuring OAM 10g

This section describes how to install and configure OAM 10g, and includes the following subsections:

- [Section 31.2.3.2.1, "Installing and Configuring OAM 10g"](#)
- [Section 31.2.3.2.2, "Installing and Configuring the Oracle HTTP Server"](#)
- [Section 31.2.3.2.3, "Configuring the WebCenter Portal Policy Domain"](#)
- [Section 31.2.3.2.4, "Installing the WebGate 10g on the WebTier"](#)

31.2.3.2.1 Installing and Configuring OAM 10g

If you don't already have Oracle Access Manager (OAM) 10g installed, install OAM 10g as described in the *Oracle Access Manager Installation Guide*.

31.2.3.2.2 Installing and Configuring the Oracle HTTP Server

If you don't already have Oracle HTTP Server (OHS) installed, install OHS (11.1.1.4.0) as described in [Section 31.2.5, "Installing and Configuring the Oracle HTTP Server."](#)

If you do have an existing installation, you will need to apply a patch to bring it up to OHS (11.1.1.4.0) as described in "Applying the Latest Oracle Fusion Middleware Patch Set" in the Oracle Fusion Middleware Patching Guide.

After installing or patching OHS, continue by installing the WebGate as described in [Section 31.2.3.2.3, "Configuring the WebCenter Portal Policy Domain."](#)

31.2.3.2.3 Configuring the WebCenter Portal Policy Domain

These steps assume that you've installed Oracle WebCenter (see WebCenter Portal). By default, an Oracle WebCenter Portal installation creates a WebLogic Server domain, including an Administration Server and four managed servers: WC_Spaces, WC_Collaboration, WC_Uutilities, and WC_Portlet.

1. 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.
2. Check that `OraDefaultExclusionAuthNScheme` is available in your OAM 10g installation. If it does not exist, create the `OraDefaultExclusionAuthNScheme` as shown below:
 - a. Open the OAM Access System Console.
 - b. Click Authentication Management.
 - c. Click Add.
 - d. Specify `OraDefaultExclusionAuthNScheme` in the Name field.
 - e. Enter `To exclude resources from being protected by OAM` in the Description field.
 - f. Enter `0` in the Level field.
 - g. Specify `None` in the Challenge Method field.
 - h. Add `unprotected:true` to the Challenge Parameter field.
 - i. Click Save.
 - j. Open the Plugins tab for this authentication scheme and click Modify.
 - k. Select `credential_mapping` from the drop down list.
 - l. Specify a value as:

```
obMappingBase="dc=us,dc=oracle,dc=com",obMappingFilter="(uid=OblixAnonymous)"
```

Make sure that this value matches the corresponding field for the `OraDefaultAnonAuthNScheme`.
 - m. Click Save.
 - n. Open the General tab again and click Modify.
 - o. Check Yes for Enabled.
 - p. Click Save.
3. Run the following command.

The `oamcfgtool.jar` is available in `ORACLE_HOME/modules/oracle.oamprovider_11.1.1/oamcfgtool.jar`

in the WebCenter Portal installation. Values in bold are the ones that you must supply based on the settings of your WebCenter Portal and OAM instances.

```
java -jar ORACLE_HOME/modules/oracle.oamprovider_11.1.1/oamcfgtool.jar
mode=CREATE app_domain=<your_domain_name>
uris_file=WEBCENTER_HOME/webcenter/scripts/webcenter.oam.conf"
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 WC_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.

4. If your instance also contains a SOA installation, then run `oamcfgtool` again to protect the SOA URIs in the policy domain you created in the previous step. Use the same parameters as the ones used in the previous step so that the existing policy domain is updated with URIs in the `soa.oam.conf` file.

```
java -jar ORACLE_HOME/modules/oracle.oamprovider_11.1.1/oamcfgtool.jar
mode=CREATE app_domain=<your_domain_name>
uris_file="SOA_HOME/soa/prov/soa.oam.conf"
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>
```

5. If your installation includes Content Server, then you also need to protect these URIs. Use the same parameters as the ones used in the previous steps so that the existing policy domain is updated with the URIs in the Content Server's `oam.conf` file.

```
java -jar ORACLE_HOME/modules/oracle.oamprovider_11.1.1/oamcfgtool.jar
mode=CREATE app_domain=<your_domain_name>
uris_file="WC_CONTENT_ORACLE_HOME/common/security/oam.conf"
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>
```

6. 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 that were specified as part of the `webcenter.oam.conf` script file. You should also see the URIs from the SOA and Content Server OAM configuration files if you have run the `oamcfgtool` from SOA and Content Server domains.
 - d. Click the domain you just created and open the Resources tab.

The URIs you specified should display. You can also open other tabs to view and verify other settings, and manually add additional resources later, if required.
7. Check the Access Gate Configurations.
 - a. Click **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 displays (it will have the suffix `_AG`), click it to see the setting details.
8. Locate the policy domain that you created and verified in the previous steps and open the Policies tab.

You should see four policies already created:

 - WebCenter REST Policy
 - Exclusion Scheme
 - Protected_JSessionId_Policy
 - Default Public Policy
9. Select `WebCenter REST Policy`, then select **Authentication Rule** and click **Modify**.
10. Change the `AuthenticationScheme` to `OraDefaultBasicAuthNScheme` (from `OraDefaultFormAuthNScheme`)
11. Go to `Exclusion Scheme policy > Authentication Rule` and check that it uses `OraDefaultExclusionAuthNScheme` (created in the previous steps) as the `AuthenticationScheme`.

12. Click **Save**.
13. Open the Policies tab and make sure that the policies are in the order shown below:

```
Protected_JSessionId_Policy
WebCenter REST Policy
Exclusion Scheme
Default Public Policy
```

14. Continue with the steps for installing the WebGate as described in [Section 31.2.3.2.4, "Installing the WebGate 10g on the WebTier."](#)

31.2.3.2.4 Installing the WebGate 10g 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. For more information, refer to the chapter on "Installing the WebGate" in the *Oracle Access Manager Installation Guide*.

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:

```
WT_ORACLE_HOME/instances/<your_instance>/config/OHS/ohs1/httpd.conf
```

Information for the AccessGate can be found in the Access System Console.

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.

5. After installing and configuring the WebGate 10g, continue by configuring the Weblogic domain as described in [Section 31.2.4, "Configuring the WebLogic Domain for OAM,"](#) and performing any additional service and component configurations that apply as described in [Section 31.2.6, "Additional Single Sign-on Configurations."](#)

31.2.4 Configuring the WebLogic Domain for OAM

If your environment spans multiple domains (for example, a domain for Spaces, a separate domain for SOA, and a separate domain for Content Server), repeat the steps in this section for each domain.

This section includes the following subsections:

- [Section 31.2.4.1, "Configuring the Oracle Internet Directory Authenticator"](#)
- [Section 31.2.4.2, "Configuring the OAM Identity Asserter"](#)
- [Section 31.2.4.3, "Configuring the Default Authenticator and Provider Order"](#)

- [Section 31.2.4.4, "Adding an OAM Single Sign-on Provider"](#)

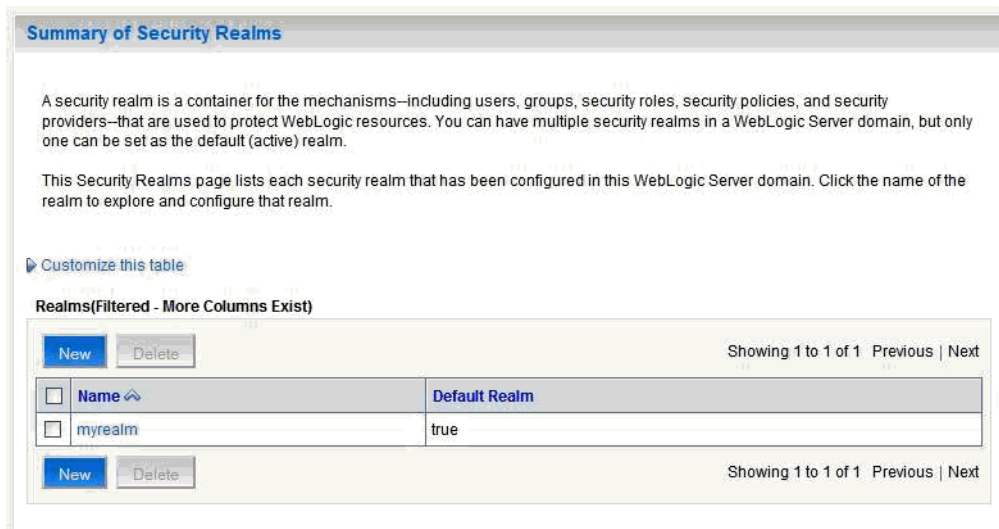
31.2.4.1 Configuring the Oracle Internet Directory Authenticator

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:

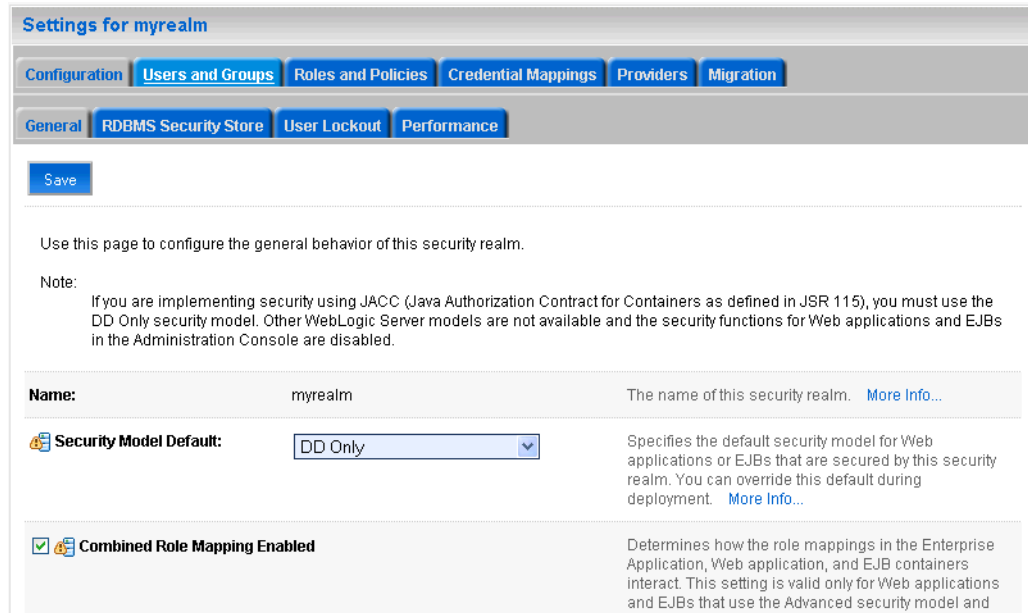
1. Log in to the WebLogic Server Administration Console.
For information on logging in to the WebLogic Server Administration Console, see [Section 1.13.2, "Oracle WebLogic Server Administration Console."](#)
2. From the Domain Structure pane, click **Security Realms**.
The Summary of Security Realms pane displays (see [Figure 31-4](#)).

Figure 31-4 Summary of Security Realms Pane



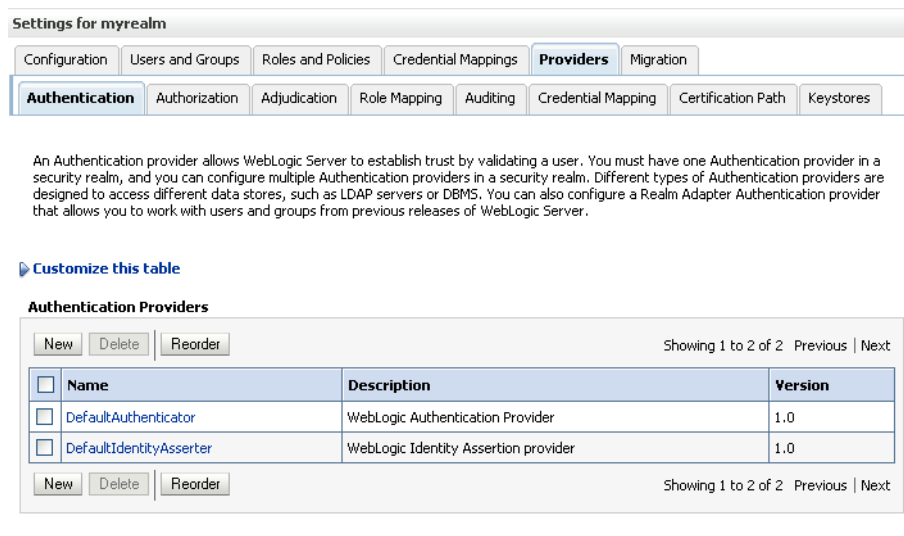
3. Click the realm entry for which to configure the OID authenticator.
The Settings pane for the realm displays (see [Figure 31-5](#)).

Figure 31–5 Settings Pane



4. Open the Providers tab.
The Provider Settings display (see [Figure 31–6](#)).

Figure 31–6 Settings Pane - Providers



5. Click **New** to create a provider.
The Create a New Authentication Provider pane displays (see [Figure 31–7](#)).

Figure 31–7 Create a New Authentication Provider Pane

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 31–8](#)).

Figure 31–8 Common Settings Pane

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 31–9](#)).

Figure 31–9 Provider Specific Settings for OID Authenticator

Settings for OID Authenticator

Configuration Performance

Common **Provider Specific**

Save

Use this page to define the provider specific configuration for this Oracle Internet Directory Authentication provider.

— Connection —

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:

SSLEnabled Specifies whether the SSL protocol should be used when connecting to the LDAP server. [More Info...](#)

— Users —

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 should be the same as for the OAM Access Manager setup
All Users Filter:	"(&(uid=*)(objectclass=person))"	

Field	Value	Comment
User Name Attribute:	"uid"	
Group Base DN:		Group search base - Same as User Base DN
Use Retrieved User Name as Principal	Checked	User login IDs are usually case insensitive. This flag is required so that the subject established contains the user name as stored in the OID.

11. Click **Save**.

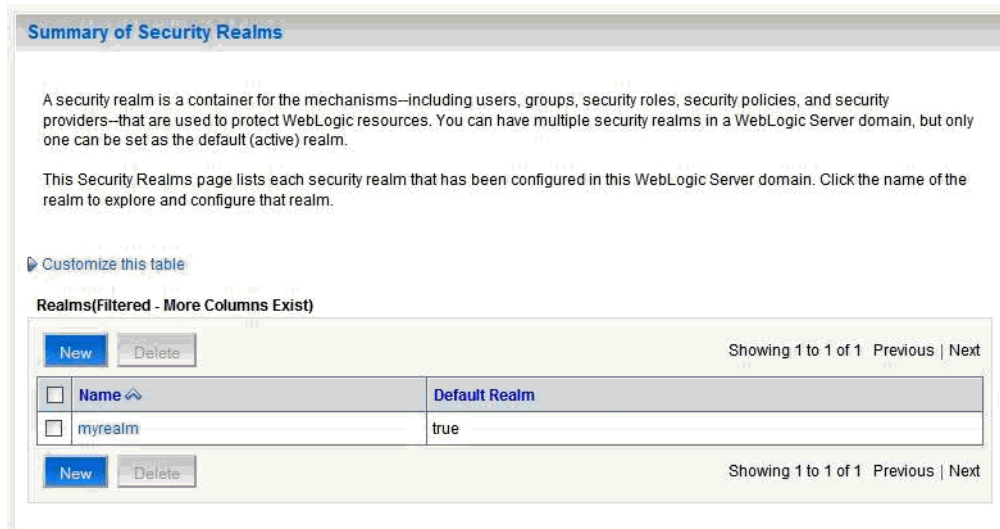
31.2.4.2 Configuring the OAM Identity Asserter

An OAM identity asserter must be configured with the provider Control Flag set to REQUIRED.

To configure the OAM Identity asserter:

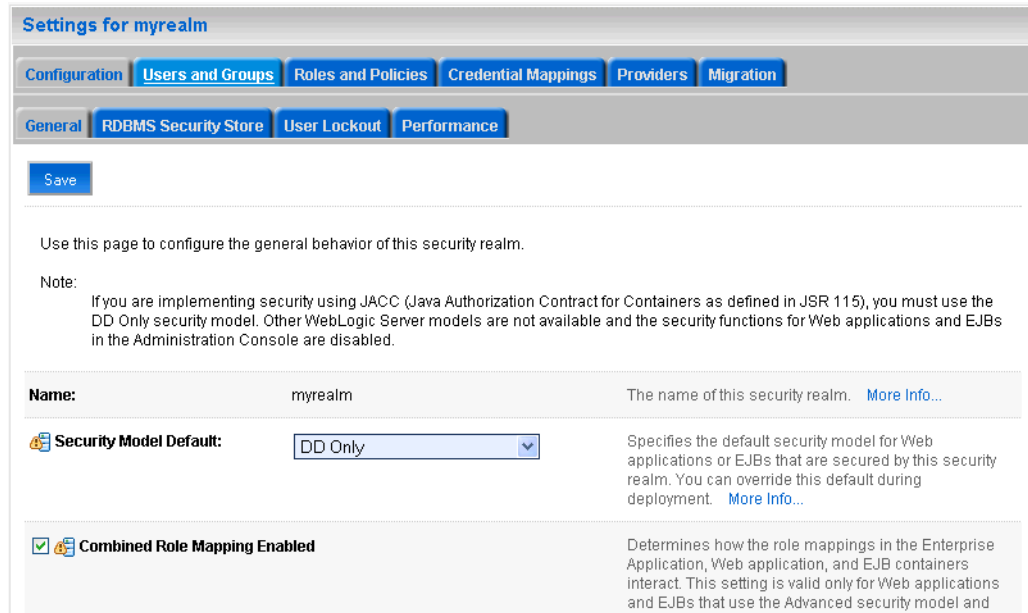
1. Log in to the WebLogic Server Administration Console.
For information on logging in to the WebLogic Server Administration Console, see [Section 1.13.2, "Oracle WebLogic Server Administration Console."](#)
2. From the Domain Structure pane, click **Security Realms**.
The Summary of Security Realms pane displays (see [Figure 31–10](#)).

Figure 31–10 Summary of Security Realms Pane



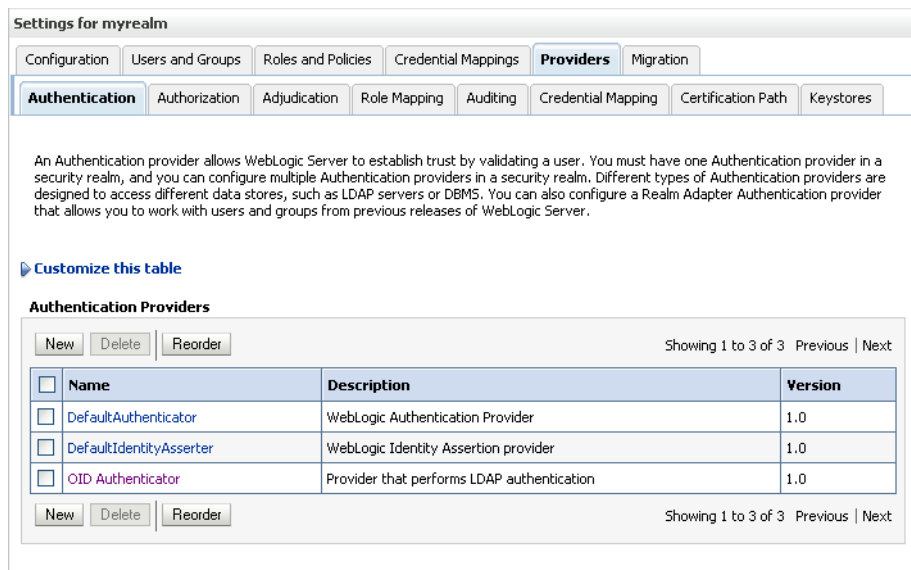
3. Click the realm entry for which to configure the OAM identity asserter.
The Settings pane for the realm displays (see [Figure 31–11](#)).

Figure 31–11 Settings Pane



4. Open the Providers tab.
The Provider Settings display (see [Figure 31–12](#)).

Figure 31–12 Settings Pane - Providers



5. Click **New** to create a provider.
The Create a New Authentication Provider pane displays (see [Figure 31–13](#)).

Figure 31–13 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 31–14](#)).

Figure 31–14 Common Settings Pane

8. Set the control flag to **REQUIRED** and check that **OAM_REMOTE_USER** and **ObSSOCookie** is set for **Active Types**.
9. Click **Save** to save you settings.

31.2.4.3 Configuring the Default Authenticator and Provider Order

After configuring the OAM identity asserter, ensure 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 31–12](#)).
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`
5. Continue by configuring Spaces for single sign-on mode as described in [Section 31.2.6.1, "Configuring WebCenter Portal: Spaces for SSO."](#) Also be sure to perform any further service and component configurations that apply to your environment as described in [Section 31.2.6, "Additional Single Sign-on Configurations."](#)

31.2.4.4 Adding an OAM Single Sign-on Provider

After checking that the default authenticator's control flag is set correctly, and that the order of the providers is correct, add an OAM SSO provider and restart all servers as described below.

Note: This is required for OAM 11g, but is only required for OAM 10g if the logout URI has been explicitly configured.

1. Connect to the WebLogic domain using WLST and run the following command:


```
addOAMSSOProvider(loginuri="/${app.context}/adfAuthentication",
logouturi="/oamssso/logout.html")
```
2. Restart all servers.

31.2.5 Installing and Configuring the Oracle HTTP Server

This step is common to both OAM 10g and OAM 11g, and should be performed after installing and configuring OAM, and before configuring the WebLogic domain.

To install and configure the Oracle HTTP server (OHS).

1. If you do not have already have an OHS install you'd like to use, install the Oracle HTTP Server (11.1.1.4.0) using the instructions in the section on *"Installing Oracle WebTier"* in the Oracle Fusion Middleware Installation Guide for Oracle Web Tier. If you do have an existing installation, you will need to apply a patch to bring it up to OHS (11.1.1.4.0) as described in *"Applying the Latest Oracle Fusion Middleware Patch Set"* in the Oracle Fusion Middleware Patching Guide.
2. Configure WebTier OHS so that it forwards requests to the Oracle WebLogic Server for WebCenter Portal using the following example in `mod_wl_ohs.conf`. Make sure that the WebLogic port numbers match your configuration. For more information, see *"Installing and Configuring Oracle HTTP Server 11g Webgate for*

OAM" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

Note: This example assumes that WebCenter Portal is a non-cluster based installation. For a clustered environment change the WebLogicHost and WebLogicPort to WeblogicCluster as required for your environment. See the section on "Installing and Configuring Oracle HTTP Server 11g Webgate for OAM" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* for details.

```
# NOTE : This is a template to configure mod_weblogic.

LoadModule weblogic_module    "${ORACLE_HOME}/ohs/modules/mod_wl_ohs.so"

# This empty block is needed to save mod_wl related configuration from EM to
# this file when changes are made at the Base Virtual Host Level
<IfModule weblogic_module>
#     WebLogicHost <WEBLOGIC_HOST>
#     WebLogicPort <WEBLOGIC_PORT>
#     Debug ON
#     WLLogFile /tmp/weblogic.log
#     MatchExpression *.jsp

<Location /webcenter>
    SetHandler weblogic-handler
    WebLogicHost webcenter.example.com
    WebLogicPort 8888
</Location>

<Location /webcenterhelp>
    SetHandler weblogic-handler
    WebLogicHost webcenter.example.com
    WebLogicPort 8888
</Location>

<Location /rss>
    SetHandler weblogic-handler
    WebLogicHost webcenter.example.com
    WebLogicPort 8888
</Location>

<Location /rest>
    SetHandler weblogic-handler
    WebLogicHost webcenter.example.com
    WebLogicPort 8888
</Location>

<Location /rsscrawl>
    SetHandler weblogic-handler
    WebLogicHost webcenter.example.com
    WebLogicPort 8888
</Location>

<Location /sesUserAuth>
    SetHandler weblogic-handler
    WebLogicHost webcenter.example.com
    WebLogicPort 8888
```

```
</Location>

<Location /owc_discussions>
  SetHandler weblogic-handler
  WebLogicHost webcenter.example.com
  WebLogicPort 8890
</Location>

<Location /activitygraph-engines>
  SetHandler weblogic-handler
  WebLogicHost webcenter.example.com
  WebLogicPort 8891
</Location>

<Location /wcps>
  SetHandler weblogic-handler
  WebLogicHost webcenter.example.com
  WebLogicPort 8891
</Location>

<Location /workflow>
  SetHandler weblogic-handler
  WebLogicHost soa.example.com
  WebLogicPort 8001
</Location>

<Location /integration/worklistapp>
  SetHandler weblogic-handler
  WebLogicHost soa.example.com
  WebLogicPort 8001
</Location>

<Location /integration/services>
  SetHandler weblogic-handler
  WebLogicHost soa.example.com
  WebLogicPort 8001
</Location>

<Location /soa-infra>
  SetHandler weblogic-handler
  WebLogicHost soa.example.com
  WebLogicPort 8001
</Location>

<Location /sdpmessaging/userprefs-ui>
  SetHandler weblogic-handler
  WebLogicHost soa.example.com
  WebLogicPort 8001
</Location>

<Location /DefaultToDoTaskFlow>
  SetHandler weblogic-handler
  WebLogicHost soa.example.com
  WebLogicPort 8001
</Location>

<Location /cs>
  SetHandler weblogic-handler
  WebLogicHost ucm.example.com
  WebLogicPort 16200
```

```
</Location>

<Location /adfAuthentication>
  SetHandler weblogic-handler
  WebLogicHost ucm.example.com
  WebLogicPort 16200
</Location>

<Location /pagelets>
  SetHandler weblogic-handler
  WebLogicHost webcenter.example.com
  WebLogicPort 8889
</Location>

<Location /services-producer>
  SetHandler weblogic-handler
  WebLogicHost webcenter.example.com
  WebLogicPort 8889
</Location>

<Location /wsrp-tools>
  SetHandler weblogic-handler
  WebLogicHost webcenter.example.com
  WebLogicPort 8889
</Location>

</IfModule>

# <Location /weblogic>
#   SetHandler weblogic-handler
#   PathTrim /weblogic
#   ErrorPage http://WEBLOGIC_HOME:WEBLOGIC_PORT/
# </Location>
```

Note: The entries in the `Location` list above map the incoming paths to the appropriate WebLogic Server managed servers on which the corresponding applications reside.

31.2.6 Additional Single Sign-on Configurations

The configurations described in the following sections may be necessary or helpful in providing additional security for your site. After completing these configurations, continue by testing your OAM installation as described in [Section 31.2.7, "Testing Your OAM Installation."](#)

- [Section 31.2.6.1, "Configuring WebCenter Portal: Spaces for SSO"](#)
- [Section 31.2.6.2, "Configuring the Discussions Server for SSO"](#)
- [Section 31.2.6.3, "Configuring the Worklist Service for SSO"](#)
- [Section 31.2.6.4, "Configuring OAM for RSS Feeds Using External Readers"](#)
- [Section 31.2.6.5, "Configuring the WebLogic Server Administration Console and Enterprise Manager for OAM 10g"](#)
- [Section 31.2.6.6, "Configuring the WebLogic Server Administration Console and Enterprise Manager for OAM 11g"](#)
- [Section 31.2.6.7, "Configuring Secure Enterprise Search for SSO"](#)

- [Section 31.2.6.8, "Configuring Content Server for SSO"](#)
- [Section 31.2.6.9, "Restricting Access with Connection Filters"](#)
- [Section 31.2.6.10, "Configuring Portlet Producers and Additional Components"](#)

31.2.6.1 Configuring WebCenter Portal: Spaces for SSO

Configure the Spaces application for SSO by adding a setting to `EXTRA_JAVA_PROPERTIES`.

There is a system property that tells WebCenter Portal 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 Portal that SSO is being used, so no login form should be displayed on the default landing page. Instead, it displays 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, and add an entry like the following:

```
EXTRA_JAVA_PROPERTIES="-Doracle.webcenter.spaces.osso=true
${EXTRA_JAVA_PROPERTIES}"
export EXTRA_JAVA_PROPERTIES
```

After making this change, restart the `WC_Spaces` server.

31.2.6.2 Configuring the Discussions Server for SSO

This section describes how to configure Oracle WebCenter Portal's Discussion Server for single sign-on. Before configuring the discussions server for SSO, ensure that it has been configured to use the same identity store LDAP as Spaces, as described in [Section 29.1, "Reassociating the Identity Store with an External LDAP Server."](#) If you've chosen not to move the default administrator account to an external LDAP, be sure to also follow the instructions in [Section 29.5.1, "Migrating WebCenter Portal's Discussions Server to Use an External LDAP."](#)

To set up the discussions server for SSO:

1. Log in to the Oracle WebCenter Portal's Discussion Server Admin Console at:

```
http://host:port/owc_discussions/admin
```

Where `host` and `port` are the host ID and port number of the `WC_Collaboration Managed Server`.

2. Open the System Properties page and edit (if it already exists) or add the `owc_discussions.sso.mode` property, setting its value to `true`.
3. Edit or add the `jiveURL` property to point to the base URL of the WebTier. For example:

```
jiveURL = webtier.example.com:7777/owc_discussions
```

The `jiveURL` property is used when constructing links to forums in emails.

31.2.6.2.1 Creating a Discussions Server Connection for Spaces

This section describes how to update the discussions server connection for Spaces so that it uses the WebTier's host and port values. Note that the steps below assume that the Discussions service has already been installed and configured in the WebCenter Portal domain.

1. Using Fusion Middleware Control or WLST, change the discussion server's URL host and port settings from the WC_Spaces Managed Server's settings, to the WebTier's host and port settings. For information about how to change these settings, see [Section 14.5, "Modifying Discussions Server Connection Details."](#)
2. Restart the WC_Spaces Managed Server.

When you log in to Spaces, you automatically sign on to the discussion server as well.

31.2.6.3 Configuring the Worklist Service for SSO

Assuming that you've already set up a Worklist connection, modify the URL to use the WebTier host and port instead of the SOA server host and port. You can do this using Fusion Middleware Control or using WLST commands as described in [Section 23.4, "Setting Up Worklist Connections."](#)

After modifying the URL and completing the setup required for OAM SSO, run the following command on the WebCenter Portal Administration server so that the Worklist service changes take effect:

```
setBPELConnection('webcenter', 'WebCenter-Worklist',
'http://webtier.example.com:7777')
```

31.2.6.4 Configuring OAM for RSS Feeds Using External Readers

By default, WebCenter Portal RSS feeds are protected by SSO. However, they will not work well with external readers if left protected. If access using external readers is important, Oracle recommends that the WebCenter Portal RSS resource be excluded from the OAM policy so that the authentication for the RSS Servlet is handled by WebLogic Server's BASIC authentication that external readers can handle.

This section contains the following subsections:

- [Section 31.2.6.4.1, "Unprotecting RSS Feeds in OAM 11g"](#)
- [Section 31.2.6.4.2, "Unprotecting RSS Feeds in OAM 10g"](#)

31.2.6.4.1 Unprotecting RSS Feeds in OAM 11g

Follow the steps below to unprotect RSS feed for OAM 11g:

1. Open the OAM Admin Console.
2. Open the Policy Configuration tab and select **Application Domain** > <your application domain>.
3. Open the Resources tab and search for `/rss*`.

Among the results, you should see:

```
/rss*
/rss/.../*
/rss/rssservlet*
/rss/rssservlet/.../*
```

4. For each resource, select the resource and click Edit.
5. Change each resource's Protection Level from Protected to Excluded and click Apply.
Note that the resource's authentication policy and authorization policy are removed.
6. Close the tab and restart OHS.

31.2.6.4.2 Unprotecting RSS Feeds in OAM 10g

Follow the steps below to unprotect RSS feed for OAM 10g:

1. Open the OAM Admin Console.
2. Select **Access System Console > Policy Manager** and open the applicable policy domain.
3. Open the Policies tab, select the `Exclusion Scheme` policy, and click Modify.
4. Select the following resources for exclusion:
 - `/rss`
 - `/rss/rssservlet`
5. Click Save.
6. Select `Default Public Policy` and click Modify.
7. Uncheck the `/rss` resource and click Save.
8. Restart OHS.

31.2.6.5 Configuring the WebLogic Server Administration Console and Enterprise Manager for OAM 10g

This section describes how to optionally set up OAM single sign-on for the WebLogic Server Administration Console and Enterprise Manager.

Note: Setting up OAM SSO for Enterprise Manager and the WebLogic Server 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 WebLogic Server Administration Console, then you may not want to complete this additional configuration step.

To set up OAM SSO for the WebLogic Server Administration Console and Enterprise Manager:

1. Log in to the OAM Console using your browser to navigate to:

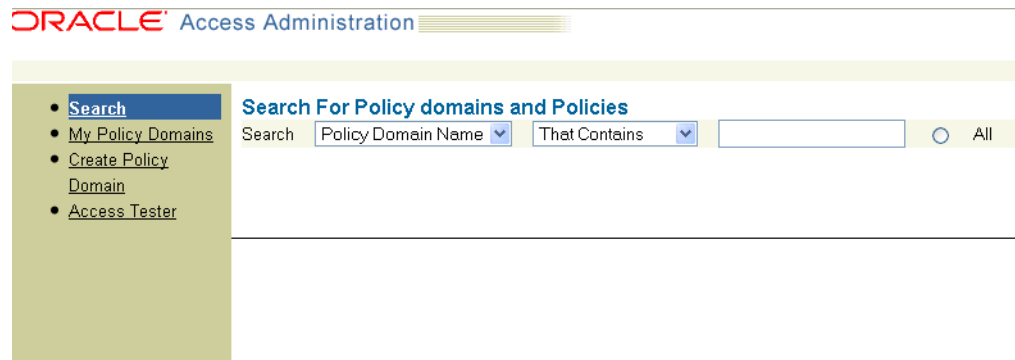
`http://host:port/access/obliz`

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**.

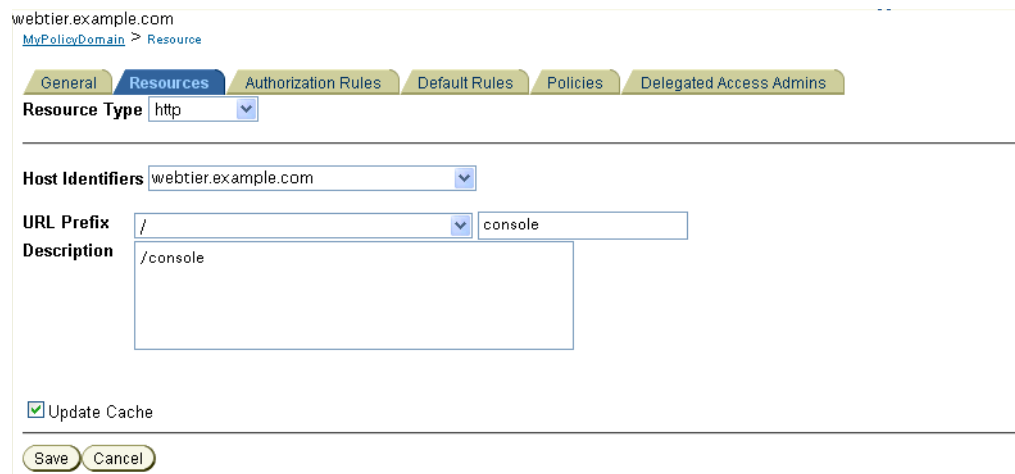
The Policy Manager pane displays (see [Figure 31-15](#)).

Figure 31–15 Policy Manager Pane



3. Locate the policy domain that you created to protect WebCenter Portal resources.
4. Open the Resources tab and click **Add**.
The Resource page displays (see Figure 31–16).

Figure 31–16 Policy Domain Resource Page



5. Add the resources that must be secured. For each resource:
 - a. Select `http` as the **Resource Type**.
 - b. Select the **Host Identifier** for the WebCenter Portal WebTier.
 - c. Enter the **URL Prefix** for the WebLogic Server Administration Console (`/console`) or Enterprise Manager (`/em`).
 - d. Enter a **Description** for the resource.
 - e. Ensure that **Update Cache** is selected, and then click **Save**.
6. In your WebTier, modify the `mod_wl_ohs.conf` file (in `WT_ORACLE_HOME/instances/<your_instance>/config/OHS/ohs1/`) to include the WebLogic Server Administration Console and Enterprise Manager, by adding two additional Location entries using the actual host ID for the WebCenter Portal Administration Server for WebLogicHost.

```
<Location /console>
    SetHandler weblogic-handler
```

```

        WebLogicHost webcenter.example.com
        WebLogicPort 7001
    </Location>

    <Location /em>
        SetHandler weblogic-handler
        WebLogicHost webcenter.example.com
        WebLogicPort 7001
    </Location>

```

- Restart the Oracle HTTP Server for your changes to take effect.

You should now be able to access the WebLogic Server 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.

31.2.6.6 Configuring the WebLogic Server Administration Console and Enterprise Manager for OAM 11g

This section describes how to optionally set up OAM 11g single sign-on for the WebLogic Server Administration Console and Enterprise Manager.

Note: Setting up OAM SSO for Enterprise Manager and the WebLogic Server 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 WebLogic Server Administration Console, then you may not want to complete this additional configuration step.

To set up OAM 11g SSO for the WebLogic Server Administration Console and Enterprise Manager:

- Log in to the OAM Console using your browser:

```
http://host:port/oamconsole
```

- Go to **Policy Configuration > Application Domains**.

The Policy Manager pane displays.

- Locate the application domain you created using the name while registering webgate agent.

- Expand the Resources node and click **Create**.

The Resource page displays.

- Add the resources that must be secured. For each resource:

- Select `http` as the **Resource Type**.
- Select the **Host Identifier** created while registering the WebGate agent.
- Enter the **Resource URL** for the WebLogic Server Administration Console (`/console`) or Enterprise Manager (`/em`).
- Enter a **Description** for the resource and click **Apply**.

6. Go to **Authentication Policies > Protected Resource Policy** and add the newly created resource.
7. Do the same under **Authorization Policies > Protected Resource Policy**.
8. In your WebTier, modify the `mod_wl_ohs.conf` file (in `WT_ORACLE_HOME/instances/<your_instance>/config/OHS/ohs1/`) to include the WebLogic Server Administration Console and Enterprise Manager, by adding two additional Location entries using the actual host ID for the WebCenter Portal Administration Server for `WebLogicHost`.

```
<Location /console>
  SetHandler weblogic-handler
  WebLogicHost webcenter.example.com
  WebLogicPort 7001
</Location>

<Location /em>
  SetHandler weblogic-handler
  WebLogicHost webcenter.example.com
  WebLogicPort 7001
</Location>
```

9. Restart the Oracle HTTP Server for your changes to take effect.

You should now be able to access the WebLogic Server 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.

31.2.6.7 Configuring Secure Enterprise Search for SSO

The crawl sources that are defined to crawl WebCenter Portal data and repositories used by WebCenter Portal and the corresponding authentication end points defined in SES must be routed through the WebTier OHS ports so that they can be properly authenticated (the authentication method continues to be BASIC and realm jazn.com). For information about configuring SES connections, see [Section 22.4, "Setting Up Oracle SES Connections."](#)

31.2.6.8 Configuring Content Server for SSO

After you've completed your SSO setup, and after setting up a connection for Content Server, specify the web context root in the `JCRContentServerConnection` using Fusion Middleware Control, or as shown in the following WLST example:

```
setJCRContentServerConnection(appName, name, webContextRoot='/cs')
```

Setting the web context root tells the Document Library code that SSO has been set up. Note that this setting should *not* be set until after SSO has been completely set up.

31.2.6.9 Restricting Access with Connection Filters

Follow the steps below to only allow users to access WebCenter Portal and other services through the WebTier OHS ports so that they can be properly authenticated.

1. Log in to the WebLogic Server Administration Console.

For information on logging in to the WebLogic Server Administration Console, see [Section 1.13.2, "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 31–17](#)).

Figure 31–17 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. You can use this information 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 WebLogic 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 Portal through the OHS port:

```
http://host:OHS_port/webcenter
```

31.2.6.10 Configuring Portlet Producers and Additional Components

If you have set up your Portlet Producer applications to route through OHS, be sure to use the OHS host and port when specifying producer URLs for registration. This applies to out-of-the-box producers like `wsrp-tools`, `services-producer`, `pagelet` producers and any other producer you have explicitly configured.

31.2.7 Testing Your OAM Installation

After installing and configuring either OAM 10g or 11g, check that you can access all of the configured applications below (as they apply to your environment), and that the global login and logout is giving you access to all of your configured applications without prompting you to sign in again. Also test global logout where available and make sure you are logged out of all other related applications.

- **Spaces:** Access any protected Spaces URL (a protected space, for example), and make sure that you see the SSO login challenge. If you are already logged into another related application that uses the same SSO, you should automatically be shown content.
- **REST:** Access `http://ohshost:ohsport/rest/api/resourceIndex`. You should see the BASIC authentication challenge. If you are already logged into another related application that uses the same SSO, you should automatically be shown content.
- **REST:** Access `http://ohshost:ohsport/rest/api/cmis/...` (retrieve this from `resourceIndex` access output in the previous step). You should not see a login challenge and should be able to see public content. When you access this after you've logged in, then you should see all content to which you have access rights.
- **ActivityGraph Engines:** Access `http://host:port/activitygraph-engines`. You should see an SSO login challenge. Once logged in, you should be able to see content.
- **Content Server:** Go to the profile UI and check that you can see Content Server screens embedded in iFrames without challenging you to log in. You should also be able to access Site Studio content in Content Presenter templates without logging in as you are already logged into Spaces application.

- **SOA:** Access links in a workflow task flow and make sure that you are not challenged to log in.
- **Discussion Forums:** Access the Discussions application at `http://host:port/owc_discussions` and log in. Check that the login is the SSO login challenge. Similarly, the Administration login to the Discussions server at `http://host:port/owc_discussions/admin` should also go through the SSO login challenge.

31.3 Configuring Oracle Single Sign-On (OSSO)

In a default installation, WebCenter Portal uses the HTTP ports in the Managed Server created for WebCenter Portal. To configure WebCenter Portal applications with Oracle Single Sign-On, WebCenter Portal needs Oracle HTTP Server and the associated Module `mod_osso` to integrate with Oracle Single Sign-On (OSSO). Note that for Framework applications some additional configurations are required, as described in [Section 32.5, "Configuring Framework Applications for OSSO."](#)

Note: The BPEL Console does not support SSO integration. When WebCenter Portal 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

- [Section 31.3.1, "Roadmap to Configuring OSSO"](#)
- [Section 31.3.2, "OSSO Components and Topology"](#)
- [Section 31.3.3, "Configuring the Oracle HTTP Server and Associated Modules"](#)
- [Section 31.3.4, "Configuring the OSSOIdentityAsserter"](#)
- [Section 31.3.5, "Registering OHS with Oracle SSO"](#)
- [Section 31.3.6, "Additional Configurations"](#)

31.3.1 Roadmap to Configuring OSSO

The flow chart ([Figure 31–18](#)) and table ([Table 31–2](#)) in this section provide an overview of the prerequisites and tasks required to configure single sign-on for WebCenter Portal using OSSO.

Figure 31–18 Configuring Single Sign-on for WebCenter Portal Using OSSO

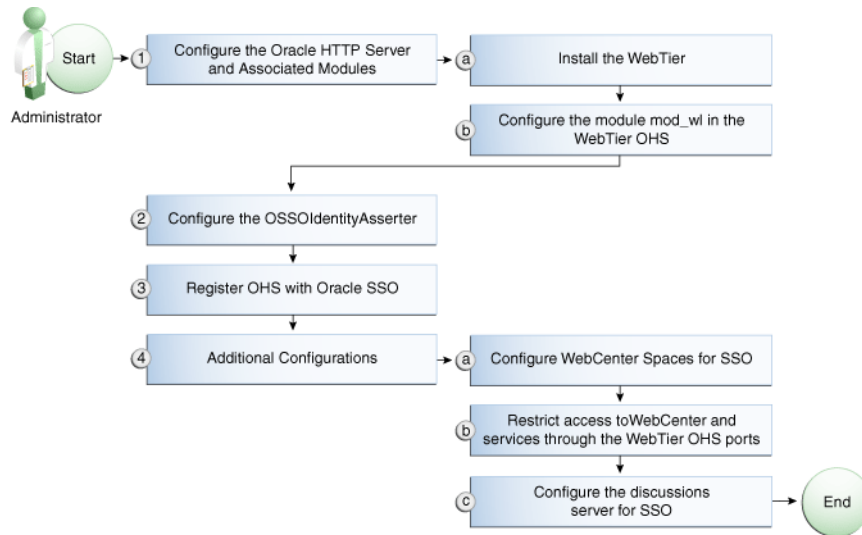


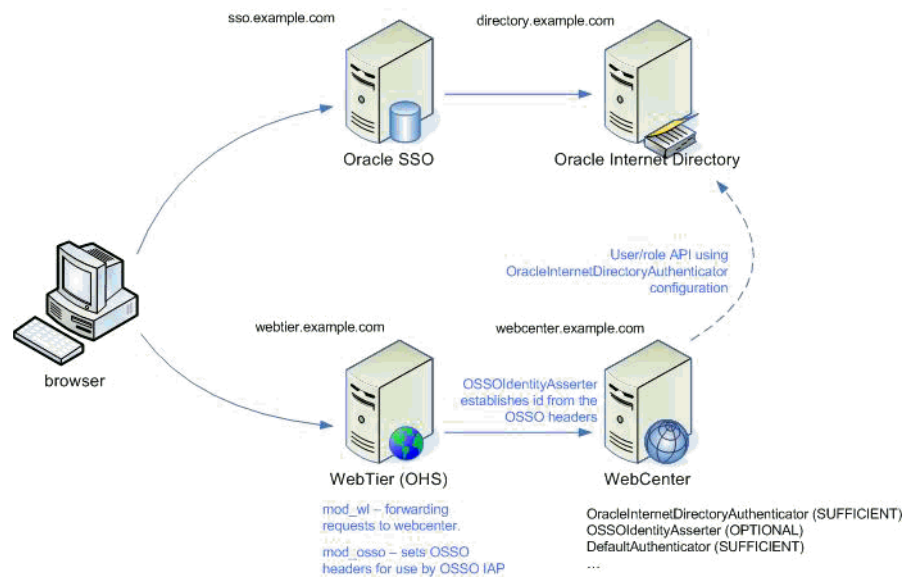
Table 31–2 shows the tasks and sub-tasks for configuring single sign-on for WebCenter Portal using OSSO.

Table 31–2 Configuring Single Sign-on for WebCenter Portal Using OSSO

Actor	Task	Sub-task	Notes
Administrator	1. Configure the Oracle HTTP Server and Associated Modules	1.a Install the WebTier	
		1.b Configure the module mod_wl in the WebTier OHS	
	2. Configure the OSSOIdentityAsserter		
	3. Register OHS with Oracle SSO		
	4. Perform additional configurations as required	4.a Configure Spaces for SSO	
		4.b Restrict access toWebCenter and services through the WebTier OHS ports	
		4.c Configure the discussions server for SSO	

31.3.2 OSSO Components and Topology

In a default installation, WebCenter Portal uses the HTTP ports of the Managed Server created for WebCenter Portal. To configure WebCenter Portal with Oracle Single Sign-On, WebCenter Portal needs the Oracle HTTP Server and the associated Module mod_osso, to integrate with Oracle SSO. The diagram below (Figure 31–19) shows the overall architecture of this integration:

Figure 31–19 OSSO Components and Topology

31.3.3 Configuring the Oracle HTTP Server and Associated Modules

This section describes how to load and configure the Oracle HTTP Server and associated modules.

To load and configure the Oracle HTTP Server and associated mods:

1. Install the Oracle WebTier software, 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 Portal, replacing the host and port values with those for your local environment.

Uncomment the lines at `${ORACLE_HOME}/ohs/modules/mod_wl_ohs.so`. This file is included by the `httpd.conf` file and looks like the following:

```
# NOTE : This is a template to configure mod_weblogic.
```

```
LoadModule weblogic_module    "${ORACLE_HOME}/ohs/modules/mod_wl_ohs.so"
```

```
# This empty block is needed to save mod_wl related configuration from EM to
this file when changes are made at the Base Virtual Host Level
```

```
<IfModule weblogic_module>
#   WebLogicHost <WEBLOGIC_HOST>
#   WebLogicPort <WEBLOGIC_PORT>
#   Debug ON
#   WLLogFile /tmp/weblogic.log
#   MatchExpression *.jsp

<Location /webcenter>
    SetHandler weblogic-handler
    WebLogicHost webcenter.example.com
    WebLogicPort 8888
</Location>

<Location /webcenterhelp>
    SetHandler weblogic-handler
```

```
        WebLogicHost webcenter.example.com
        WebLogicPort 8888
    </Location>

    <Location /rss>
        SetHandler weblogic-handler
        WebLogicHost webcenter.example.com
        WebLogicPort 8888
    </Location>

    <Location /rest>
        SetHandler weblogic-handler
        WebLogicHost webcenter.example.com
        WebLogicPort 8888
    </Location>

    <Location /rsscrawl>
        SetHandler weblogic-handler
        WebLogicHost webcenter.example.com
        WebLogicPort 8888
    </Location>

    <Location /sesUserAuth>
        SetHandler weblogic-handler
        WebLogicHost webcenter.example.com
        WebLogicPort 8888
    </Location>

    <Location /services-producer>
        SetHandler weblogic-handler
        WebLogicHost webcenter.example.com
        WebLogicPort 8889
    </Location>

    <Location /wsrp-tools>
        SetHandler weblogic-handler
        WebLogicHost webcenter.example.com
        WebLogicPort 8889
    </Location>

    <Location /owc_discussions>
        SetHandler weblogic-handler
        WebLogicHost webcenter.example.com
        WebLogicPort 8890
    </Location>

    <Location /activitygraph-engines>
        SetHandler weblogic-handler
        WebLogicHost webcenter.example.com
        WebLogicPort 8891
    </Location>

    <Location /wcps>
        SetHandler weblogic-handler
        WebLogicHost webcenter.example.com
        WebLogicPort 8891
    </Location>

    <Location /workflow>
        SetHandler weblogic-handler
```

```

        WebLogicHost soa.example.com
        WebLogicPort 8001
    </Location>

    <Location /integration/worklistapp>
        SetHandler weblogic-handler
        WebLogicHost soa.example.com
        WebLogicPort 8001
    </Location>

    <Location /integration/services>
        SetHandler weblogic-handler
        WebLogicHost soa.example.com
        WebLogicPort 8001
    </Location>

    <Location /soa-infra>
        SetHandler weblogic-handler
        WebLogicHost soa.example.com
        WebLogicPort 8001
    </Location>

    <Location /sdpmessaging/userprefs-ui>
        SetHandler weblogic-handler
        WebLogicHost soa.example.com
        WebLogicPort 8001
    </Location>

    <Location /DefaultToDoTaskFlow>
        SetHandler weblogic-handler
        WebLogicHost soa.example.com
        WebLogicPort 8001
    </Location>

    <Location /cs>
        SetHandler weblogic-handler
        WebLogicHost ucm.example.com
        WebLogicPort 16200
    </Location>

    <Location /adfAuthentication>
        SetHandler weblogic-handler
        WebLogicHost ucm.example.com
        WebLogicPort 16200
    </Location>

</IfModule>

# <Location /weblogic>
#     SetHandler weblogic-handler
#     PathTrim /weblogic
#     ErrorPage http://WEBLOGIC_HOME:WEBLOGIC_PORT/
# </Location>

```

31.3.4 Configuring the OSSOIdentityAsserter

Include the OSSO Identity Assertion Provider (IAP) provider in the Oracle WebLogic domain for WebCenter Portal. Use the WebLogic Server Administration Console to

add the OSSO IAP to your domain as shown in the steps below. If your environment spans multiple domains (for example, a domain for Spaces, separate domain for SOA, and a separate domain for Content Server), repeat the steps in this section for each domain.

To configure the OSSOIdentityAsserter:

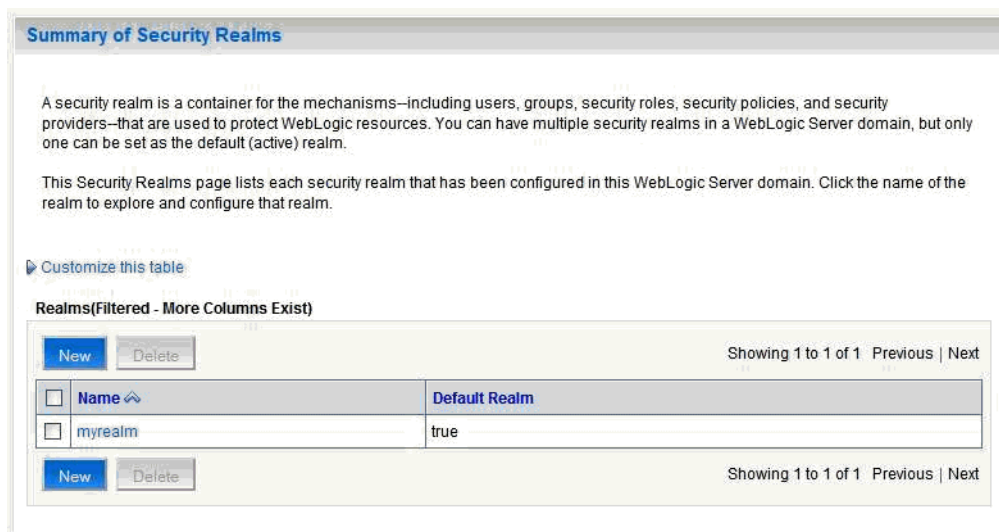
1. Log in to the WebLogic Server Administration Console.

For information on logging in to the WebLogic Server Administration Console, see [Section 1.13.2, "Oracle WebLogic Server Administration Console."](#)

2. From the Domain Structure pane, click **Security Realms**.

The Summary of Security Realms pane displays (see [Figure 31–20](#)).

Figure 31–20 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 31–21](#)).

Figure 31–21 Settings Pane

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

4. Click the Providers tab.

The Provider Settings display (see [Figure 31–22](#)).

Figure 31–22 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 provider.

The Create a New Authentication Provider pane displays (see [Figure 31–23](#)).

Figure 31–23 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. Ensure that **OracleInternetDirectoryAuthenticator** (or the primary authenticator you selected when you configured the Identity Store to use an external LDAP) is set as the primary authenticator for the domain so that the user profile can be retrieved from the associated Oracle Internet Directory server. For information about configuring the Identity Store to use an external LDAP, see [Chapter 29, "Configuring the Identity Store."](#)

For OID, the provider list should appear as follows:

- **OSSOIdentityAsserter** (OPTIONAL)
- **OracleInternetDirectoryAuthenticator** (SUFFICIENT)
- **DefaultAuthenticator** (SUFFICIENT)
- **DefaultIdentityAsserter** (OPTIONAL)

31.3.5 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 FTP it in binary mode to the WebTier host (`WT_ORACLE_HOME`).

The following example shows how you would register a remote partner application on a SSO Server. Check that the `ORACLE_HOME` environment variable is set (`ORACLE_HOME` here is the `ORACLE_HOME` of the OSSO installation on the SSO server) before running `ssoreg.sh`.

```
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:80 -remote_midtier -config_file
```



```
webtier.example.com.osso.conf
```

Running this command creates a `webtier.example.com.osso.conf` file.

2. Copy the

`WT_ORACLE_HOME/instances/<your_instance>/config/OHS/ohs1/disabled/mod_osso.conf` file to

`WT_ORACLE_HOME/instances/<your_instance>/config/OHS/ohs1/moduleconf`. All files in the `moduleconf` directory are included in the `httpd.conf` file.

- ## 3. Copy the `webtier.example.com.osso.conf` file generated by `ssoreg` in **step 1** to a location accessible in the WebTier other than the `moduleconf` directory (for example, `WT_ORACLE_HOME`).

Note: If using FTP, be sure to transfer the file using binary mode.

- ## 4. Add rules to the `mod_osso.conf` file to protect the `/webcenter` and related application resources URLs with Oracle SSO.

The `mod_osso.conf` file should look similar to this:

```
LoadModule osso_module "${ORACLE_HOME}/ohs/modules/mod_osso.so"
```

```
<IfModule osso_module>
    OsoIpCheck off
    OsoIdleTimeout off
    OsoSecureCookies Off

#Point to proper osso.conf file.
    OsoConfigFile /scratch/pyarashi/ohs/dadvmi0003.osso.conf
#
# Insert Protected Resources: (see Notes below for
# how to protect resources)
#
#_____ -
#
# Notes
#
#_____ -
#
# 1. Here's what you need to add to protect a resource,
#    e.g. <ApacheServerRoot>/htdocs/private:
#
#    <Location /private>
#        require valid-user
#        AuthType Osso
#    </Location>

    <Location /webcenter/adfAuthentication*>
        OsoSendCacheHeaders off
        require valid-user
        AuthType Osso
    </Location>
    <Location /services-producer/adfAuthentication*>
        OsoSendCacheHeaders 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 /integration/worklistapp>
  OssoSendCacheHeaders off
  require valid-user
  AuthType Osso
</Location>
<Location /sdpmessaging/userprefs-ui>
  OssoSendCacheHeaders off
  require valid-user
  AuthType Osso
</Location>
<Location /workflow/WebCenterWorklistDetail>
  OssoSendCacheHeaders off
  require valid-user
  AuthType Osso
</Location>
<Location /workflow/sdpmessaging-sca-ui-worklist>
  OssoSendCacheHeaders off
  require valid-user
  AuthType Osso
</Location>
<Location /rest/api/resourceIndex>
  OssoSendCacheHeaders off
  require valid-user
  AuthType Osso
</Location>
<Location /rest/api/spaces>
  OssoSendCacheHeaders off
  require valid-user
  AuthType Osso
</Location>
<Location /rest/api/discussions>
  OssoSendCacheHeaders off
  require valid-user
  AuthType Osso
</Location>

```

```
<Location /rest/api/tags>
  OsoSendCacheHeaders off
  require valid-user
  AuthType Oso
</Location>
<Location /rest/api/taggeditems>
  OsoSendCacheHeaders off
  require valid-user
  AuthType Oso
</Location>
<Location /rest/api/activities>
  OsoSendCacheHeaders off
  require valid-user
  AuthType Oso
</Location>
<Location /rest/api/activitygraph>
  OsoSendCacheHeaders off
  require valid-user
  AuthType Oso
</Location>
<Location /rest/api/feedback>
  OsoSendCacheHeaders off
  require valid-user
  AuthType Oso
</Location>
<Location /rest/api/people>
  OsoSendCacheHeaders off
  require valid-user
  AuthType Oso
</Location>
<Location /rest/api/messageBoards>
  OsoSendCacheHeaders off
  require valid-user
  AuthType Oso
</Location>
<Location /rest/api/searchresults>
  OsoSendCacheHeaders off
  require valid-user
  AuthType Oso
</Location>
<Location /pagelets/admin>
  OsoSendCacheHeaders off
  require valid-user
  AuthType Oso
</Location>
<Location /pagelets/authenticateWithApplicationServer*>
  OsoSendCacheHeaders off
  require valid-user
  AuthType Oso
</Location>
<Location /activitygraph-engines>
  OsoSendCacheHeaders off
  require activity-graph-admins
  AuthType Oso
</Location>
<Location /wcps/api>
  OsoSendCacheHeaders off
  require valid-user
  AuthType Oso
</Location>
```

```

    <Location /cs/groups>
        OssoSendCacheHeaders off
        require valid-user
        AuthType Osso
    </Location>
    <Location /cs/idcplg>
        OssoSendCacheHeaders off
        require valid-user
        AuthType Osso
    </Location>
    <Location /adfAuthentication>
        OssoSendCacheHeaders off
        require valid-user
        AuthType Osso
    </Location>
</IfModule>

#
# To have short hostnames redirected to fully qualified
# hostnames for clients that need authentication via
# mod_osso to be able to enter short hostnames into their
# browsers use a mod_rewrite configuration such as the following.
#
# e.g
#RewriteEngine On
#RewriteCond %{HTTP_HOST} !www.example.com
#RewriteRule ^.*$
http://%{SERVER_NAME}%{REQUEST_URI}
[R]
#where www.example.com is the fully qualified domain name.

```

Be sure to change the **OssoConfigFile** parameter to point to the location (and filename if you've changed it) where you copied your `osso.conf` file in the previous step. If your environment is non-SSL, then also be sure to turn off OSSO secure cookies (on by default):

```
OssoSecureCookies Off
```

- Restart the WebTier so that the configuration changes to `mod_osso` and `mod_wl` take effect.

31.3.6 Additional Configurations

The configurations described in the following sections may be necessary or helpful in providing additional security for your site. For Framework applications the additional configurations described in [Section 32.5, "Configuring Framework Applications for OSSO"](#) are also required.

- [Section 31.3.6.1, "Configuring WebCenter Portal: Spaces for SSO"](#)
- [Section 31.3.6.2, "Restricting Access Using the WebTier OHS Ports"](#)
- [Section 31.3.6.3, "Configuring the Discussions Server for SSO"](#)
- [Section 31.3.6.4, "Configuring the Worklist Service for SSO"](#)
- [Section 31.3.6.5, "Configuring Oracle Content Server for SSO"](#)
- [Section 31.3.6.6, "Configuring OSSO for RSS Feeds Using External Readers"](#)
- [Section 31.3.6.7, "Configuring SES Crawl for SSO"](#)

31.3.6.1 Configuring WebCenter Portal: Spaces for SSO

Complete the configuration for Oracle Single Sign-on (OSSO) for Spaces by adding a setting to `EXTRA_JAVA_PROPERTIES` and rebooting as described in [Section 31.2.6.1, "Configuring WebCenter Portal: Spaces for SSO."](#)

31.3.6.2 Restricting Access Using the WebTier OHS Ports

To only allow users to access WebCenter Portal and other services through the WebTier OHS ports so that they can be properly authenticated, follow the steps in [Section 31.2.6.9, "Restricting Access with Connection Filters."](#)

31.3.6.3 Configuring the Discussions Server for SSO

This section describes how to configure Oracle WebCenter Portal's Discussion Server for single sign-on. Before configuring the discussions server for SSO, ensure that it has been configured to use the same identity store LDAP as Spaces, as described in [Section 29.5.1, "Migrating WebCenter Portal's Discussions Server to Use an External LDAP."](#)

To set up the discussions server for SSO:

1. Log in to the Oracle WebCenter Portal's Discussion Server Admin Console at:

```
http://host:port/owc_discussions/admin
```

Where *host* and *port* are the host ID and port number of the WC_Collaboration Managed Server.

2. Open the System Properties page and edit (if it already exists) or add the `owc_discussions.sso.mode` property, setting its value to `true`.
3. Update the `jiveURL` property to point to the base URL of the WebTier.

31.3.6.4 Configuring the Worklist Service for SSO

After registering OHS with Oracle SSO, as shown in [Section 31.3.5, "Registering OHS with Oracle SSO,"](#) run the following command on the WebCenter Portal Administration server so that the Worklist service changes to take effect:

```
setBPPELConnection('webcenter', 'WebCenter-Worklist',
'http://webtier.example.com:7777')
```

31.3.6.5 Configuring Oracle Content Server for SSO

Since it's possible to access the Content Server repository directly from Spaces, you may also want to include it in the single sign-on configuration. Assuming that you've already set up a connection for the Content Server, specify the web context root in the `JCRContentServerConnection` using Fusion Middleware Control or using WLST as shown in the following example:

```
setJCRContentServerConnection(appName, name, webContextRoot='/cs')
```

For more information on how to configure the Content Server, see "Configuring Content Server to Use Single Sign-On" in the *Oracle WebCenter Content System Administrator's Guide for Content Server*.

31.3.6.6 Configuring OSSO for RSS Feeds Using External Readers

By default, WebCenter Portal RSS feeds are protected by SSO. However, they will not work well with external readers if left protected. If access using external readers is

important, Oracle recommends that the WebCenter Portal RSS resource be unprotected so that the authentication for the RSS Servlet is handled by WebLogic Server's BASIC authentication that external readers can handle.

Follow the steps below to unprotect the RSS feeds:

1. Remove the following entry from `mod_osso.conf`.

```
<Location /rss/rssservlet>
  OssoSendCacheHeaders off
  require valid-user
  AuthType Osso
</Location>
```

2. Restart OHS.

31.3.6.7 Configuring SES Crawl for SSO

If you have SES configured for your instance, you can optionally update the WebCenter Portal Crawl and authentication end points to use the WebTier URL. See [Chapter 22, "Managing Oracle SES Search in WebCenter Portal"](#) for more information.

31.4 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 for all WebCenter Portal applications other than Pagelet Producer applications. 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. Note that since Pagelet Producer applications do not participate in SAML SSO, users are required to log in explicitly if they access the Pagelet Producer application. Note also that for Framework applications, some additional configurations are required as described in [Section 32.6, "Configuring Framework Applications for SAML SSO."](#)

Note: Although SAML-based single sign-on provides support for logging users onto subsequent applications after initial sign-on, global logout is not supported. Consequently, users must log out of each individual application they open.

Note also that if you set up SAML-based single sign-on with Spaces as the source application and Discussions as the destination application, administrators can access the Discussions administration pages from Spaces Administration (**Configuration > Services**) and Space Settings (Services page). However, since Discussions administration pages do not participate in SSO, if you access administration pages directly, you are required to log in to the Discussions server again.

Finally, SAML-based single sign-on is not available for the `sdpMessaging userprefs-ui` application. As an application administrator, if you click **Manage Configuration** in the **Preferences > Messaging** dialog in Spaces, you will need to log in again.

This SSO mechanism can be used for departmental WebCenter Portal installations for which there is no existing Oracle SSO or Oracle Access Manager single sign-on infrastructure, but single sign-on between only 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 WebCenter Portal: Spaces and the Worklist service running on different managed servers within the same domain.

This section includes the following subsections:

- [Section 31.4.1, "SAML Components and Topology"](#)
- [Section 31.4.2, "Configuring SAML-based Single Sign-on"](#)

31.4.1 SAML Components and Topology

[Figure 31–25](#) shows the components and their interaction in a SAML-based single sign-on configuration that includes Spaces and the Discussions 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 31–24](#) shows the components and flow for a POST-configured SAML SSO configuration that includes both a WebCenter Portal and SOA domain. The flow is similar for other destination applications participating in single sign-on such as Worklist applications and Discussions.

Figure 31–24 Detailed SAML Single Sign-on Components and Topology (POST Profile Configured)

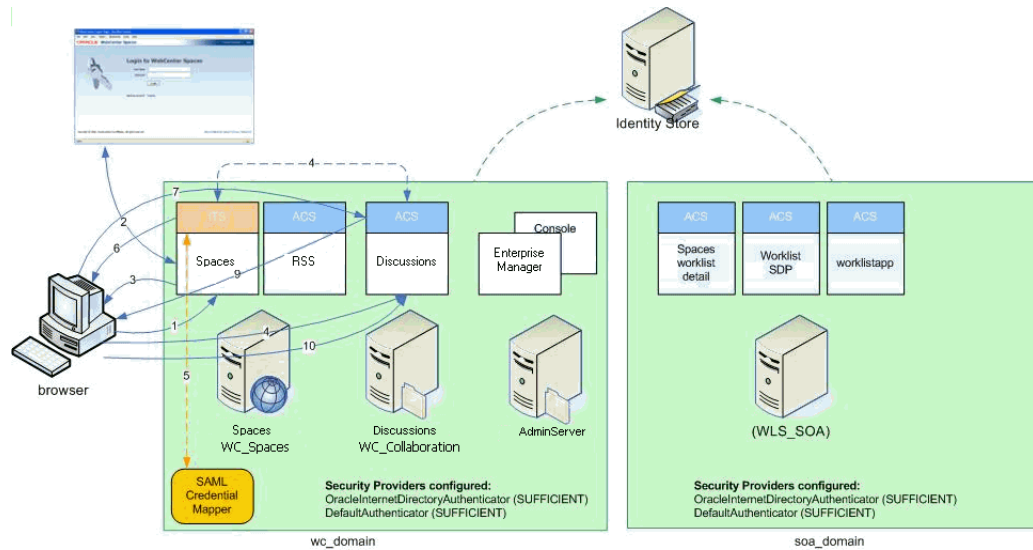
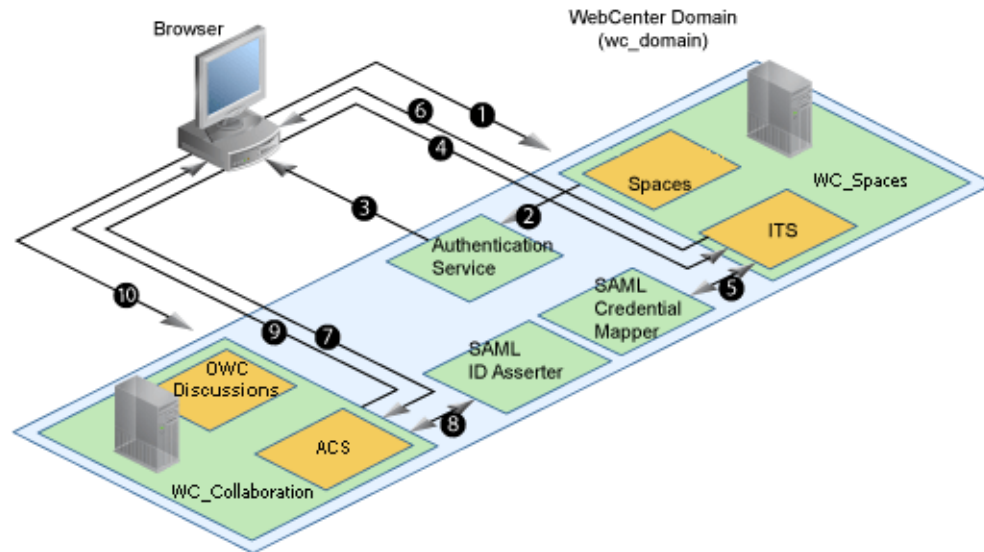


Figure 31–25 shows a simplified version of the components and flow for a POST-configured SAML SSO configuration, including the SAML SSO flow between Spaces and the Discussions application.

Figure 31–25 SAML Single Sign-on Components and Topology (POST Profile Configured)



The steps in the flow are:

1. The user's browser accesses Spaces (source site), hosted on a WebLogic managed server (WC_Spaces) in the WebCenter Portal domain (wc_domain), by supplying user credentials.
2. Spaces passes the user credentials to the authentication service provider.
3. If authentication is successful, the authenticated session is established, and the 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 Discussions service (destination site), hosted on a different WebLogic Server (`wc_collaboration`) 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 Spaces application on the `wc_spaces` Managed Server) that shares the same JSESSIONID cookie as Spaces.
5. The ITS servlet calls the SAML Credential Mapper configured in the WebCenter Portal 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 Discussions 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 Discussions 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 Discussions service).
10. The user is logged in on the destination site Discussions service without having to reauthenticate.

31.4.2 Configuring SAML-based Single Sign-on

This section describes how to configure Spaces and services for SAML-based single sign-on using a set of automated scripts.

This section includes the following subsections:

- [Section 31.4.2.1, "SAML Single Sign-on Prerequisites"](#)
- [Section 31.4.2.2, "Configuring SAML-based SSO"](#)
- [Section 31.4.2.3, "Configuring SAML SSO for RSS Using External Readers"](#)
- [Section 31.4.2.4, "Checking Your Configuration"](#)
- [Section 31.4.2.5, "Disabling Your SAML SSO Configuration"](#)
- [Section 31.4.2.6, "Removing Your SAML SSO Configuration"](#)

31.4.2.1 SAML Single Sign-on Prerequisites

This section describes a set of steps that should be carried out prior to configuring SAML-based single sign-on. Note that these steps assume that Spaces and associated components are already installed and the relevant connections have been configured and tested.

The prerequisites for SAML-based SSO are described in the following subsections:

- [Section 31.4.2.1.1, "Configuring Oracle Content Server for SAML SSO"](#)
- [Section 31.4.2.1.2, "Configuring the Discussions Server for SAML SSO"](#)
- [Section 31.4.2.1.3, "Configuring and Exporting the Certificates"](#)

- [Section 31.4.2.1.4, "Setting Up SSL"](#)

31.4.2.1.1 Configuring Oracle Content Server for SAML SSO

If your instance uses a Documents connection that requires the use of OHS to surface the Content Server user interface in WebCenter Portal, you need to configure WebCenter Portal and related applications with a WebTier.

When configuring SAML SSO for a configuration that includes Content Server, all HTTP URLs should point to the WebTier host and port. Additionally when Content Server is front-ended with OHS, the following entries must appear in `mod_wl_ohs.conf`, apart from the usual configuration for WebCenter Portal:

```
<Location /cs>
    SetHandler weblogic-handler
    WebLogicHost ucm.example.com
    WebLogicPort 16200
</Location>

<Location /adfAuthentication>
    SetHandler weblogic-handler
    WebLogicHost ucm.example.com
    WebLogicPort 16200
</Location>

<Location /samlacs/acs>
    SetHandler weblogic-handler
    WebLogicHost ucm.example.com
    WebLogicPort 16200
</Location>
```

See [Section 31.2.5, "Installing and Configuring the Oracle HTTP Server"](#) for more information about installing OHS and editing `mod_wl_ohs.conf`.

Additionally, when a custom login page is used for Spaces the following HTML comment must be added to the head section of the HTML page generated for Content Server for Site Studio Designer to work:

```
<!--IdcClientLoginForm=1-->
```

This HTML comment appears in the out-of-the-box log in pages in Spaces, but if you configure a new page to be the login page in a SAML SSO setup, then the comment must be added by hand, or in generated HTML as shown in the following example for a JSF page:

```
<af:document id="d1">
    <f:facet name="metaContainer">
        <f:verbatim>
            ${cb.commentText}
        </f:verbatim>
    </f:facet>
    .....
```

where `cb` is a managed bean containing the method:

```
public String getCommentText(){
    return "<!--IdcClientLoginForm=1-->";
}
```

After checking that the comment text is added verbatim in the `metaContainer` facet of `af:document`, check the generated HTML page using View Source and confirm that `<!--IdcClientLoginForm=1-->` is in the `<head>` section of the HTML page.

31.4.2.1.2 Configuring the Discussions Server for SAML SSO

By default, the .EAR file that is deployed for the Oracle WebCenter Portal's Discussion Server Server supports form-based Oracle SSO or Oracle Access Manager SSO. Therefore, before you can configure the Oracle WebCenter Portal's Discussion Server Server for SAML-based single sign-on, you must also first deploy the SAML SSO version of the discussion server .EAR file.

Note: Before configuring the discussions server for SSO, ensure that it is configured to use the same identity store LDAP as Spaces, as described in [Section 29.1, "Reassociating the Identity Store with an External LDAP Server."](#) If you've chosen not to move the default administrator account to an external LDAP, be sure to also follow the instructions in [Section 29.5.1, "Migrating WebCenter Portal's Discussions Server to Use an External LDAP."](#)

To deploy and configure the SAML SSO version of the Oracle WebCenter Portal's Discussion Server Server:

1. Log in to the WebLogic Server Administration Console as an administrator.

For information on logging in to the WebLogic Server Administration Console, see [Section 1.13.2, "Oracle WebLogic Server Administration Console."](#)

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

The Deployments Summary pane displays (see [Figure 31–26](#)).

Figure 31–26 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 (`owc_discussions_samlssso.ear`, typically in `$WC_ORACLE_HOME/discussionserver`).

5. Select the `owc_discussions_saml_sso.ear` file and click **Next**.
6. Select **Install this deployment as an application** and click **Next**.
7. Set the **Name** to `owc_discussions`.
8. Deploy the `.EAR` file.
9. Log in to the Discussions Server Administration Console as an administrator (see [Section 31.2.6.2, "Configuring the Discussions Server for SSO"](#) for more information on logging in to the Discussions Server Administration Console).
10. Open the System Properties page and edit (if it already exists) or add the `owc_discussions.sso.mode` property, setting its value to `true`.
11. Restart the `WC_Collaboration` Managed Server (where the discussions server is deployed).

31.4.2.1.3 Configuring and Exporting the Certificates

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 WebLogic Server Administration Console.

To create certificates using `keytool`:

1. Configure the necessary keystore for the `WC_Spaces` and Administration servers in the WebCenter Portal domain. This keystore should contain the certificate you intend to use for securing the SAML assertions.

If you only want to test the configuration, you can either create a "demoidentity" certificate that is packaged in the `DemoIdentity` keystore that is configured by default, or you can use `keytool` to generate a new certificate in the `DemoIdentity` keystore. For more information about configuring a custom identity keystore, see [Section 33.1.2, "Configuring the Custom Identity and Java Trust Keystores."](#)

2. Using `keytool`, export the certificate you have chosen to use to encrypt SAML assertions. Be sure to run the `export` command on the keystore that is configured for `WC_Spaces` and the Administration server for the Spaces domain.

```
keytool -export -keystore <keystore_name> -storepass <keystore_password> -alias
<certificate_alias> -keypass <certificate_password> -file <certificate.der>
```

where:

- `keystore_name` is the name of the keystore that is configured for `WC_Spaces` and the Administration server for the Spaces domain
- `keystore_password` is the password of the keystore that is configured for `WC_Spaces` and the Administration server for the Spaces domain
- `certificate_alias` is the alias name (for example, `demoidentity`)
- `certificate_password` is the password for the certificate
- `certificate.der` is the name of the certificate file

Note that the `keytool -export` command should be run from the Spaces machine and should export the certificate being used in the SAML SSO setup residing in the keystore configured for the Spaces server.

3. Copy or transfer the file into the destination domains (such as SOA, Content Server, and Collaboration) and configure the `certPath` value in the `wcsamlssso.properties` file when you are ready to run the SAML SSO script as described in [Section 31.4.2.2.1, "The Single Sign-on Script."](#)

31.4.2.1.4 Setting Up SSL

If the WebCenter Portal installation requires SSL for providing transport-level security, then SSL should be configured before configuring single sign-on as described in [Chapter 33, "Configuring SSL."](#) Note that setting up SSL is not related to enabling SSO.

31.4.2.2 Configuring SAML-based SSO

After installing Spaces and services as required for your environment, continue by configuring SAML-based single sign-on using the scripts as described in this section.

The scripts set up SAML-based single sign-on in a WebLogic environment by configuring:

- SAML Credential Mapping Provider
- Necessary relying parties
- Source Site Federation Services
- SAML Identity Asserter
- Necessary asserting parties
- Destination Site Federation Services

This section includes the following subsections:

- [Section 31.4.2.2.1, "The Single Sign-on Script"](#)
- [Section 31.4.2.2.2, "Using the Scripts"](#)

31.4.2.2.1 The Single Sign-on Script

The single sign-on script to configure SAML 1.1 SSO for Spaces and related applications is located in the `$WC_ORACLE_HOME/webcenter/scripts/samlssso` folder. The following files are relevant for SAML configuration:

- [wcsamlssso.properties](#)
- [wcsamlssso.py](#)
- [configureSpaces.py](#)
- [configureCollab.py](#)
- [configureUtilities.py](#)
- [configureSOA.py](#)
- [configureUCM.py](#)
- [configureREST.py](#)
- [configureForum.py](#)
- [configureActivityGraphEngine.py](#)
- [configureWorklistIntegration.py](#)
- [configureWorklistDetail.py](#)

- [configureWorklistSDP.py](#)
- [configureCS.py](#)

wcsamlssso.properties

This properties file (`$WC_ORACLE_HOME/common/bin/wcsamlssso.properties`) encapsulates the necessary configuration information for the SAML SSO setup. The properties file has the following sections:

spaces_config

This section captures the login information, WebLogic Admin URL, Spaces server and URL, and so forth, of the WebCenter Portal domain required for the Credential Mapper and Source Site Federation Services configuration. All properties in this section must be completed.

- `configFile` - Config file containing the weblogic user account and password for the WebCenter Portal domain
- `keyFile` - Key file to decrypt the weblogic user account and password for the WebCenter Portal domain
- `adminURL` - WebLogic Admin URL to connect to WLST
- `usesSSL` - Indicates whether Spaces is configured to use SSL
- `url` - WebCenter Portal URL. If `usesSSL` is "true", then change "http" to "https". If Spaces is front-ended with WebTier, then specify the WebTier host and port here.
- `serverName` - Server where Spaces is deployed, typically `WC_Collaboration`
- `certAlias` - Alias of certificate to sign SAML assertions
- `certPassword` - Encrypted password of certificate to sign SAML assertions

collab_config

This section captures the login information, admin URL, certificate file path, and so forth, of the Collaboration domain required for the Identity Asserter and Destination Site Federation Services configuration. Only complete this section if your setup has Discussions configured.

- `configFile` - Config file containing weblogic user account and password for the Services domain
- `keyFile` - Key file to decrypt weblogic user account and password for the Services domain
- `adminURL` - WebLogic Admin URL to connect to WLST
- `usesSSL` - Indicates whether Discussions service is configured to use SSL
- `serverName` - Server where Discussions is deployed (typically the `WC_Collaboration Managed Server`)
- `certAlias` - Alias of certificate to verify SAML assertions
- `certPath` - Path to exported certificate to verify SAML assertions. Note that the certificate path should be a valid path on the machine that hosts the domain (i.e., the one specified in `adminURL`)

utilities_config

This section captures the login information, admin URL, and certificate file path of the Utilities domain required for the Identity Asserter and Destination Site Federation

Services configuration. Complete this section out only if your setup is configured with the Activity Graph application.

- `configFile` - Config file containing `weblogic` user account and password for the Utilities domain
- `keyFile` - Key file to decrypt `weblogic` user account and password for the Utilities domain
- `adminURL` - WebLogic Admin URL to connect to WLST
- `usesSSL` - Indicates whether Utilities applications are configured to use SSL
- `serverName` - Server where Utilities applications are deployed (typically the `WC_Utilities` Managed Server)
- `certAlias` - Alias of certificate to verify SAML assertions
- `certPath` - Path to exported certificate to verify SAML assertions. Note that the certificate path should be a valid path on the machine that hosts the domain (i.e., the one specified in `adminURL`)

soa_config

This section captures the login information, admin URL, certificate file path, and so forth, of the SOA domain required for the Identity Asserter and Destination Site Federation Services configuration. Only complete this section if your setup has SOA configured.

- `configFile` - Config File containing the `weblogic` user account and password for the SOA domain
- `keyFile` - Key File to decrypt the `weblogic` user account and password for the SOA domain
- `adminURL` - WebLogic Admin URL to connect to WLST
- `usesSSL` - Indicates whether SOA applications are configured to use SSL
- `serverName` - Server where SOA applications are deployed (typically `soa_server1`)
- `certAlias` - Alias of certificate to verify SAML assertions
- `certPath` - Path to exported certificate to verify SAML assertions. Note that the certificate path should be a valid path on the machine that hosts the domain (i.e., the one specified in `adminURL`)

ucm_config

This section captures the login information, admin URL, certificate file path, and so forth, of the Content Server domain required for the Identity Asserter and Destination Site Federation Services configuration. Only complete this section if your installation has the Documents service configured.

- `configFile` - Config file containing the `weblogic` user name and password for the Content Server (UCM) domain
- `usesSSL` - Indicates whether Content Server applications are configured to use SSL
- `keyFile` - Key File to decrypt the `weblogic` user account and password for the Content Server (UCM) domain
- `adminURL` - WebLogic Administration URL to connect to WLST

- `serverName` - Server where Content Server applications are deployed (typically `UCM_server1`)
- `certPath` - Path to exported certificate to verify SAML assertions. Note that the certificate path should be a valid path on the machine that hosts the domain (i.e., the one specified in `adminURL`)

rss_config

This is mandatory

- `url` - RSS URL. If `usesSSL` in `spaces_config` is "true", then change "http" to "https". If RSS is front-ended with WebTier, then specify the WebTier host and port here.

rest_config

This section must be completed.

- `url` - REST URL. If `usesSSL` in `spaces_config` is "true", then change "http" to "https". If REST is front-ended with WebTier, then specify the WebTier host and port here.

forum_config

Complete this section if your configuration has Discussions installed.

- `url` - OWC Discussions URL. If `usesSSL` in `collab_config` is "true", then change "http" to "https". If Discussions is front-ended with WebTier, then specify the WebTier host and port here.

worklist_config

Complete this section of SOA is installed and Worklist is configured for Spaces.

- `worklist_detail` - Worklist Detail application URL. If `usesSSL` in `soa_config` is "true", then change "http" to "https". If Worklist Detail application is front-ended with WebTier, then specify the WebTier host and port here.
- `worklist_sdp` - Worklist SDP application URL. If `usesSSL` in `soa_config` is "true", then change "http" to "https". If Worklist Detail application is front-ended with WebTier, then specify the WebTier host and port here.
- `worklist_integration` - Worklist Integration application URL. If `usesSSL` in `soa_config` is "true", then change "http" to "https". If Worklist Detail application is front-ended with WebTier, then specify the WebTier host and port here.

activitygraph_config

Complete this section if your configuration has the Utilities server installed.

- `url` - ActivityGraphEngines URL. If `usesSSL` in `spaces_config` is "true", then change "http" to "https". If the Activity Graph application is front-ended with WebTier, then specify the WebTier host and port here.

cs_config

Complete this section if your configuration has Content Server installed and you have a Documents service connection configured for the Spaces application.

- `url` - Content Server URL. If `usesSSL` in `spaces_config` is "true", then change "http" to "https". If Content Server is front-ended with WebTier, then specify the WebTier host and port here. Note that if both Spaces and Content Server are configured for your environment, then they must both be accessed using the same WebTier.

wcsamlssso.py

Script file (`$WC_ORACLE_HOME/common/wlst/wcsamlssso.py`) that contains utility functions invoked by rest of the configuration scripts

configureSpaces.py

Executable script

(`$WC_ORACLE_HOME/webcenter/scripts/samlssso/configureSpaces.py`) to configure SAML 1.1 Credential Mapper, SAML 1.1 Identity Asserter and Source and Destination site federation services on the WebCenter Portal domain

configureCollab.py

Executable script

(`$WC_ORACLE_HOME/webcenter/scripts/samlssso/configureCollab.py`) to configure SAML 1.1 Identity Asserter and Destination site federation services on the Collaboration domain

configureUtilities.py

Executable script

(`$WC_ORACLE_HOME/webcenter/scripts/samlssso/configureUtilities.py`) to configure SAML 1.1 Identity Asserter and Destination site federation services on the Utilities domain

configureSOA.py

Executable script

(`$WC_ORACLE_HOME/webcenter/scripts/samlssso/configureSOA.py`) to configure SAML 1.1 Identity Asserter and Destination site federation services on the SOA domain

configureUCM.py

Executable script

(`$WC_ORACLE_HOME/webcenter/scripts/samlssso/configureUCM.py`) to configure SAML 1.1 Identity Asserter and Destination site federation services on the Content Server domain

configureREST.py

Executable script

(`$WC_ORACLE_HOME/webcenter/scripts/samlssso/configureREST.py`) to configure asserting and relying parties for the REST application

configureRSS.py

Executable script

(`$WC_ORACLE_HOME/webcenter/scripts/samlssso/configureRSS.py`) to configure asserting and relying parties for RSS

application

configureForum.py

Executable script

(`$WC_ORACLE_HOME/webcenter/scripts/samlssso/configureForum.py`) to configure asserting and relying parties for the Discussions application

configureActivityGraphEngine.py

Executable script

(\$WC_ORACLE_HOME/webcenter/scripts/samlssso/configureActivityGraphEngine.py) to configure asserting and relying parties for the Activity Graph Engine application

configureWorklistIntegration.py

Executable script

(\$WC_ORACLE_HOME/webcenter/scripts/samlssso/configureWorklistIntegration.py) to configure asserting and relying parties for the Worklist Integration application

configureWorklistDetail.py

Executable script

(\$WC_ORACLE_HOME/webcenter/scripts/samlssso/configureWorklistDetail.py) to configure asserting and relying parties for the Worklist Community Detail application

configureWorklistSDP.py

Executable script

(\$WC_ORACLE_HOME/webcenter/scripts/samlssso/configureWorklistSDP.py) to configure asserting and relying parties for the Worklist SDP application

configureCS.py

Executable script

(\$WC_ORACLE_HOME/webcenter/scripts/samlssso/configureCS.py) to configure asserting and relying parties for the Content Server application.

31.4.2.2.2 Using the Scripts

Follow the steps below to use the scripts to configure SAML-based single sign-on:

Note: If you encounter errors when running the scripts due to configuration errors, the SAML SSO configuration may be left in an incomplete state. The config scripts provided are not rerunnable; you must clean up the SAML SSO artifacts before you retry the configuration as described in [Section 31.4.2.6, "Removing Your SAML SSO Configuration."](#)

1. Ensure that the Administration server for all the domains used in this configuration are up and running.
2. Generate the config and key files containing the connection information for the various domains using the `storeUserConfig` WLST command from the `$WC_ORACLE_HOME/common/bin` so that the `properties` file is picked up. Use the command-line help (`help('storeUserConfig')`) for usage and syntax details.
 - a. Connect using WLST to the WebCenter Portal domain using the admin username and password, and run the following command:

```
storeUserConfig('spacesconfig.secure', 'spaceskey.secure')
```

This creates a user configuration file and an associated key file. The user configuration file contains an encrypted username and password. The key file contains a secret key that is used to encrypt and decrypt the username and

password. The above command stores the config and key files in the directory from where WLST was invoked, or you can optionally specify a more secure path.

- b. Repeat step 2a after connecting to the Collaboration domain using the admin username and password. Even if the Utilities server is in the same domain as Spaces (`wc_domain`), you must connect to the WebCenter Portal domain and run this command:

```
storeUserConfig('collabconfig.secure',
'collabkeykey.secure')
```

- c. Repeat step 2a after connecting to the Utilities domain using the admin username and password. Even if the Utilities server is in the same domain as Spaces (`wc_domain`), you must connect to the WebCenter Portal domain and run this command:

```
storeUserConfig('utilitiesconfig.secure',
'utilitieskey.secure')
```

- d. Repeat step 2a after connecting to the SOA domain using the admin username and password. Even if SOA is installed on the same domain as Spaces, you must connect to the WebCenter Portal domain and run this command:

```
storeUserConfig('soaconfig.secure', 'soakey.secure')
```

- e. Repeat step 2a after connecting to the Content Server domain using the admin username and password.

```
storeUserConfig('ucmconfig.secure', 'ucmkey.secure')
```

3. Launch WLST and run the WLST `encrypt` command to encrypt the certificate password. Use the command-line help (`help('encrypt')`) for usage and syntax details.

```
print encrypt(obj='<certificatePassword>', domainDir='<full
path to the Spaces domain directory>')
```

This displays the encrypted certificate password. The `encrypt` command uses the encryption for a specified WebLogic Server domain root directory. The encrypted output needs to be set as the `certPassword` value in `wcsamlssso.properties` mentioned in the next step. Since this password will be set onto the credential mapper and source site federation services in the WebCenter Portal domain, ensure that you run the encryption utility from the WebCenter Portal domain.

4. Edit `$WC_ORACLE_HOME/common/bin/wcsamlssso.properties` and complete the sections applicable to your setup. Refer to [Section 31.4.2.2.1, "The Single Sign-on Script"](#) for a detailed description of the sections in the properties file.
5. Launch WLST from `$WC_ORACLE_HOME/common/bin` and execute the scripts in the order shown below.

Note: Run the scripts in the WLST offline mode as the scripts include an explicit connect command.

- a. `execfile('<wc_oracle_home>/webcenter/scripts/samlssso/configureSpaces.py')`

Restart all servers including the Administration server in the WebCenter Portal domain.

- b. If you have a discussions server set up, execute the `configureCollab.py` script:

```
execfile('<wc_oracle_home>/webcenter/scripts/samlssso/configureCollab.py')
```

If Discussions belongs to the same domain as Spaces, then only restart the WC_Collaboration Managed Server. Otherwise, restart all servers including the Administration server in the Collaboration domain.

- c. If you have a Utilities server set up, execute the `configureUtilities.py` script:

```
execfile('<wc_oracle_home>/webcenter/scripts/samlssso/configureUtilities.py')
```

If the Utilities server belongs to the same domain as Spaces, then only restart the WC_Utilities server. Otherwise, restart all servers including the Administration server in the Utilities domain.

- d. If you have Worklist configured for Spaces, execute the `configureSOA.py` script:

```
execfile('<wc_oracle_home>/webcenter/scripts/samlssso/configureSOA.py')
```

Restart all servers including the Administration server in the SOA domain.

- e. If you have the Documents service configured for Spaces, run the `configureUCM.py` script as shown below:

```
execfile('<wc_oracle_home>/webcenter/scripts/samlssso/configureUCM.py')
```

Restart all servers including the Administration server in the Content Server domain.

6. Run the individual commands below as required for your environment.

```
execfile('<wc_oracle_home>/webcenter/scripts/samlssso/configureREST.py') - No restart is required.
```

```
execfile('<wc_oracle_home>/webcenter/scripts/samlssso/configureRSS.py') - No restart is required.
```

```
execfile('<wc_oracle_home>/webcenter/scripts/samlssso/configureForum.py') - Do this if you have Discussions installed in your setup. No restart is required.
```

```
execfile('<wc_oracle_home>/webcenter/scripts/samlssso/configureActivityGraphEngine.py') - Do this if you have Utilities installed in your setup. No restart is required.
```

```
execfile('<wc_oracle_home>/webcenter/scripts/samlssso/configureWorklistIntegration.py') - Do this if you have Worklist installed in your setup. No restart is required.
```

```
execfile('<wc_oracle_home>/webcenter/scripts/samlssso/configureWorklistDetail.py') - Do this if you have Worklist installed in your setup. No restart is required.
```

```
execfile('<wc_oracle_home>/webcenter/scripts/samlssso/configureWorklistSDP.py') - Do this if you have Worklist installed in your setup. No restart is required.
```

`execfile('<wc_oracle_home>/webcenter/scripts/samlssso/configureCS.py')` - Do this if you have Content Server installed in your setup. No restart is required.

7. Check your installation using the steps provided in [Section 31.4.2.4, "Checking Your Configuration."](#)

IMPORTANT: Since the properties file contains sensitive information, delete it from `$WC_ORACLE_HOME/common/bin` after you have configured and verified the SAML SSO setup. Also delete the config and key files you generated in **step 2** above.

Note: If you encounter errors when running the scripts, you must remove the asserting and relying parties set up by the scripts before running the scripts again as described in [Section 31.4.2.6, "Removing Your SAML SSO Configuration."](#)

After removing your old SAML SSO configuration, continue by re-running the scripts.

31.4.2.3 Configuring SAML SSO for RSS Using External Readers

By default, WebCenter Portal RSS feeds are protected by SSO. However, they will not work well with external readers if left protected. If access using external readers is important, Oracle recommends that the WebCenter Portal RSS resource be unprotected so that the authentication for the RSS Servlet is handled by WebLogic Server's BASIC authentication that external readers can handle.

Follow the steps below to unprotect the RSS feeds:

1. Log onto the WLS Administration Console for the Spaces domain.
2. Open the security realm and select **Providers > Credential Mapping > wcsamlcm > Management > Relying Parties**.
3. Disable or delete the relying party for RSS.
4. Open the security realm and select **Providers > Authentication > wcsamlia > Management > Asserting Parties**.
5. Disable or delete the asserting party for RSS.

31.4.2.4 Checking Your Configuration

Follow the steps below to check that your single sign-on configuration is working correctly.

To test your single sign-on configuration:

1. Using a new browser, log in to Spaces and check that you're not challenged for credentials when you click **Forum Administration** from **Space Settings > Services > Discussions** (assuming this service is provisioned for the space).
2. Access the RSS link from Discussions or WorkList task flow, and check that you are not challenged to log in.
3. For Content Server, go to the Profile user interface and make sure you see Content Server screens embedded in iFrames without being challenged to log in. You should also be able to access Site Studio content in Content Presenter templates without being challenged to log in as you are already logged into Spaces.

4. Access `http://host:port/rest/api/resourceIndex` and make sure you see the BASIC authentication challenge. If you are already logged in to another related application that uses the same SSO, you should shown content without being challenged to log in.
5. To test SOA, access links in the Workflow task flow and make sure you are not challenged to log in.

If while testing SAML SSO you encounter 404 or 403 errors, check the SAML configuration and also turn on debug logging for SAML on the AdminServer. Also turn on logging for the WC_Spaces server and the server hosting your destination site. The logs will be available in

`$domain.home/servers/<server>/logs/<server>.log`. For information on how to turn on logging for WC_Spaces and other application servers, see [Section 38.3, "Viewing and Configuring Log Information."](#) Before re-running the scripts, remove your SAML SSO configuration as described in [Section 31.4.2.6, "Removing Your SAML SSO Configuration."](#)

31.4.2.5 Disabling Your SAML SSO Configuration

This section describes how to temporarily disable your SAML SSO configuration for testing or other purposes.

To disable your SAML SSO configuration:

1. Log onto the WLS Administration Console for the Spaces domain.
2. Open the security realm and select **Providers > Credential Mapping > wcsamlcm > Management > Relying Parties** and diable all the relying parties shown there.
3. Open the security realm and select **Providers > Authentication > wcsamlia > Management > Asserting Parties** and disable all the asserting parties shown there.
4. If there are other WLS domains, such as SOA or Content Server, that have been configured with SAML SSO, remove the SAML SSO configuration from these domains as well:
 - a. Log in to the WLS Administration Console for the WLS domain.
 - b. Open the security realm and select **Providers > Authentication > wcsamlia > Management > Asserting Parties** and disable all the asserting parties shown there.
5. Confirm that the SAML SSO configuration has been disable by opening your applications and checking that you are not prompted to sign in.

31.4.2.6 Removing Your SAML SSO Configuration

Since the SAML SSO configuration scripts do not include a cleanup facility, if you have made errors while updating the `wcsaml.sso.properties` file or running the scripts, the configuration could be in an invalid state. At this point, it's better to clean up all the SAML SSO configurations and start over. This section describes the steps to remove the SAML SSO configuration.

Note that if you have fully set up SAML SSO (i.e., the script ran to completion), then all the instructions below will be valid. However, if you encountered errors while running the script, then the configuration may be incomplete and only some of the artifacts below will be present and will need to be removed.

To remove your SAML SSO configuration:

1. Log onto the WLS Administration Console for the Spaces domain.

2. Open the security realm and select **Providers > Credential Mapping > wcsamlcm > Management > Relying Parties** and delete all the relying parties shown there.
3. Open the security realm and select **Providers > Authentication > wcsamlia > Management > Asserting Parties** and delete all the asserting parties shown there.
4. Go to **Providers > Authentication > wcsamlia > Management > Certificates** and delete the certificate there.
5. Go to **Providers > Credential Mapping > wcsamlcm** and delete the SAML Credential Mapper.
6. Go to **Providers > Authentication > wcsamlia** and delete the SAML Identity Asserter.
7. Restart the entire Spaces WLS domain.
8. If there are other WLS domains, such as SOA or Content Server, that have been configured with SAML SSO, remove the SAML SSO configuration from these domains as well:
 - a. Log in to the WLS Administration Console for the WLS domain.
 - b. Open the security realm and select **Providers > Authentication > wcsamlia > Management > Asserting Parties** and delete all the asserting parties shown there.
 - c. Go to **Providers > Authentication > wcsamlia > Management > Certificates** and delete the certificate there.
 - d. Go to **Providers > Authentication > wcsamlia** and delete the SAML Identity Asserter.
 - e. Restart the entire WLS domain.
9. Confirm that the SAML SSO configuration has been removed by opening your applications and checking that you are not prompted to sign in. You can now safely use the scripts again to reconfigure SAML SSO.

31.5 Configuring SSO for Microsoft Clients

This section describes how to set up single sign-on (SSO) for 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 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 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) must parse SPNEGO tokens in order to extract Kerberos tokens, which are then used for authentication.

This section contains the following subsections:

- [Section 31.5.1, "Microsoft Client SSO Concepts"](#)
- [Section 31.5.2, "System Requirements"](#)
- [Section 31.5.3, "Configuring Microsoft Clients"](#)

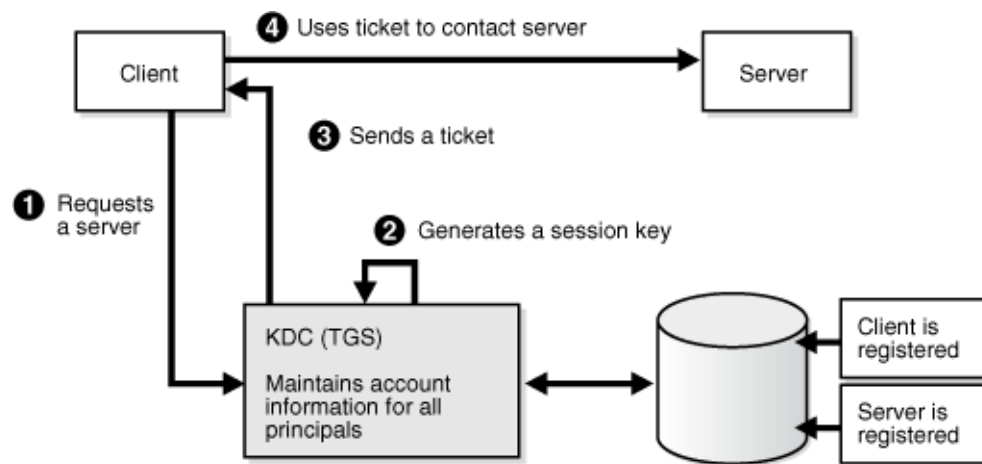
31.5.1 Microsoft Client SSO Concepts

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 31–27 Connecting to a Server Through a Key Distribution Center

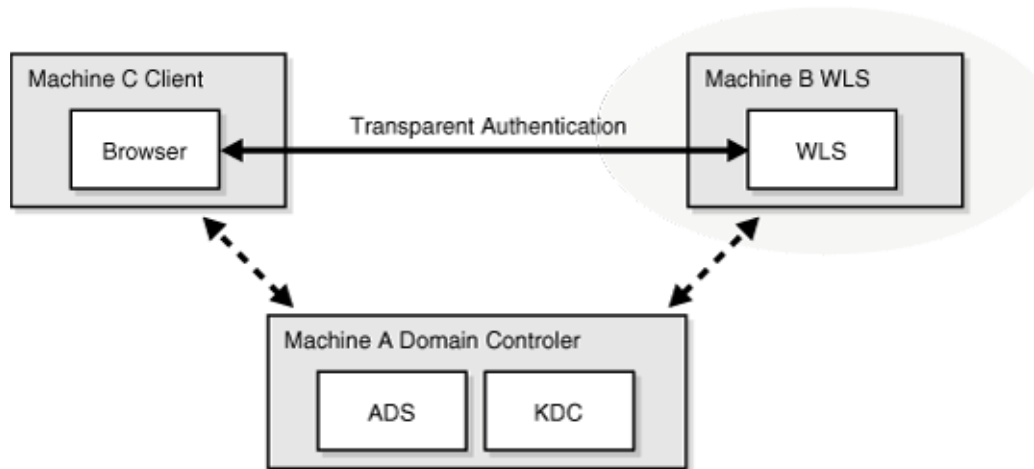


Understanding SPNEGO

SPNEGO (Simple and Protected GSSAPI Negotiation Mechanism) is a GSSAPI "pseudo mechanism" that is used to negotiate one of several 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 WebLogic Server, and to transparently provide the WebLogic Server with authentication information from the Kerberos database using a SPNEGO ticket. The WebLogic Server can recognize the ticket and extract the information from it. WebLogic Server 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 WebLogic Server.)

Figure 31–28 SPNEGO-based Authentication

31.5.2 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

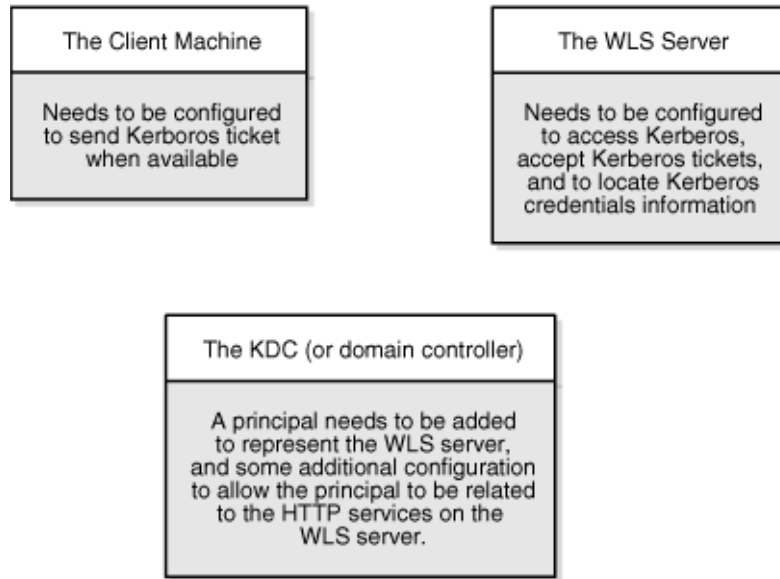
Client systems with:

- 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.

31.5.3 Configuring Microsoft Clients

Configuring SSO with Microsoft clients requires configuring the Microsoft Active Directory, the Microsoft client, and the WebLogic Server domain shown in [Figure 31–29](#). For detailed configuration steps and troubleshooting, see "Configuring Single Sign-On with Microsoft Clients" in *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

Figure 31–29 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 (see "Configuring Single Sign-On with Microsoft Clients" in the *Oracle Fusion Middleware Securing Oracle WebLogic Server*).
3. Choose a browser client (Internet Explorer or Mozilla Firefox) and configure it to use Windows Integrated authentication see ("Configuring Microsoft Clients to Use Windows Integrated Authentication" in the *Oracle Fusion Middleware Securing Oracle WebLogic Server*.)
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 (see "Creating a JAAS Login File" in *Oracle Fusion Middleware Securing Oracle WebLogic Server*).
 - b. Configure a Negotiate Identity Assertion provider in the WebLogic Server security realm (see [Section 31.5.3.1, "Configuring the Negotiate Identity Assertion Provider"](#)).
 - c. Configure the WebLogic Server 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 31.5.3.2, "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. Add the following system properties to the `JAVA_OPTIONS` in `setDomainEnv.sh` for each WebCenter Portal machine, changing the values below for the values of the particular host (on one line):

```
-Dnon_sso_protocol=http
-Dnon_sso_host=example.com
-Dnon_sso_port=8888
-Dsso_base_url=http://example.com:7777
```

The `non_sso` values are the value on the machine for protocol, host, and port. The `sso` values are the value that the user would see when directed through OHS.

6. For WebCenter Portal: Spaces, configure the WebTier OHS so that it forwards requests to the Oracle WebLogic Server for WebCenter Portal, as described in [Section 31.6, "Configuring SSO with Virtual Hosts."](#)
7. Restart the WebLogic Servers (Administration Server and managed servers) using the startup arguments specified in step 5. Repeat steps 4, 5, and 6 for the SOA domain to enable single sign-on for SOA applications.
8. Restart the OHS for the changes to take effect.
9. Configure the discussions server (see [Section 31.5.3.4, "Configuring the Discussions Server for SSO"](#)).

31.5.3.1 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 through Kerberos.

To configure the Negotiate Identity Assertion provider:

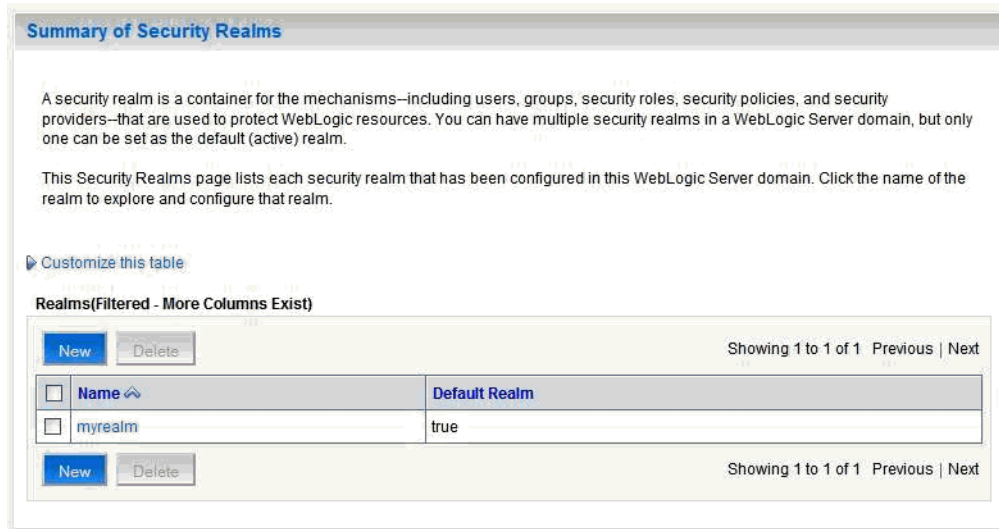
1. Log in to the WebLogic Server Administration Console.

For information on logging in to the WebLogic Server Administration Console, see [Section 1.13.2, "Oracle WebLogic Server Administration Console."](#)

2. From the Domain Structure pane, click **Security Realms**.

The Summary of Security Realms pane displays (see [Figure 31–30](#)).

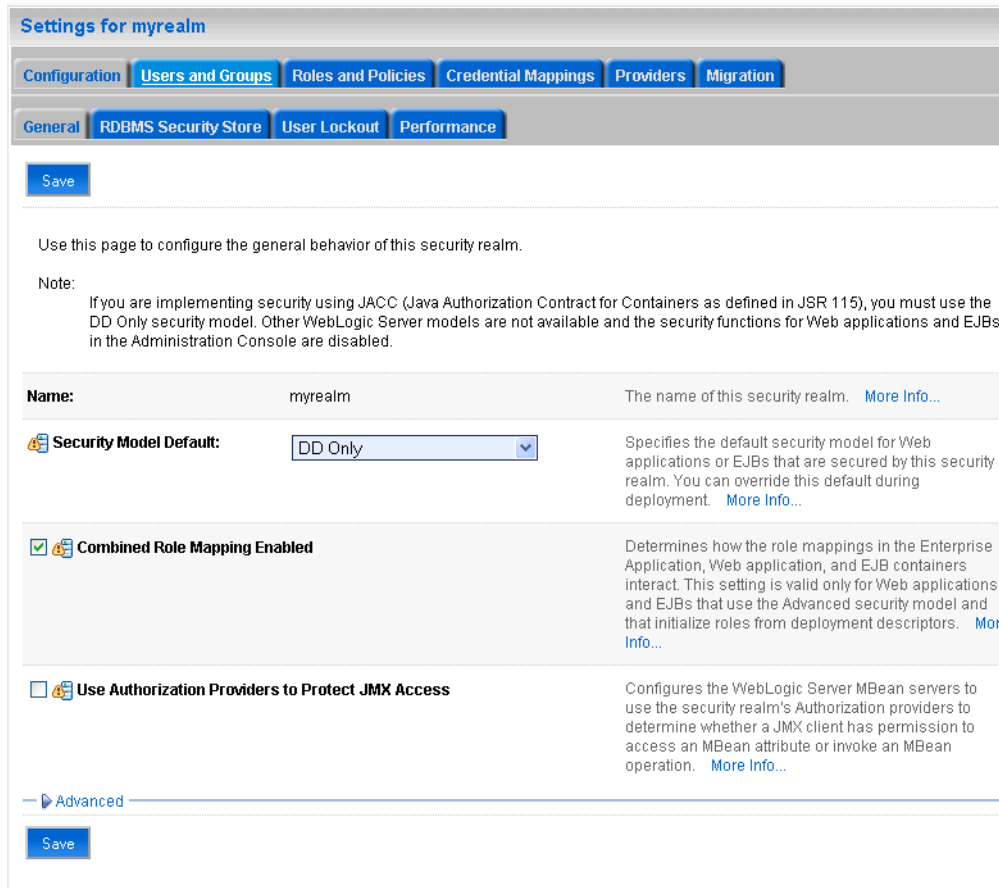
Figure 31–30 Summary of Security Realms Pane



3. Click your security realm.

The Settings page for the security realm displays (see [Figure 31–31](#)).

Figure 31–31 Security Realm Settings Page



- Open the Providers tab and select the Authentication subtab.
The Authentication Settings pane displays (see [Figure 31–32](#)).

Figure 31–32 Authentication 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

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

- Click **New**.
The Create a New Authentication Provider pane displays (see [Figure 31–33](#)).

Figure 31–33 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

- Enter a **Name** for the identity asserter, and select `NegotiateIdentityAsserter` as the **Type**.
- Click **OK**.

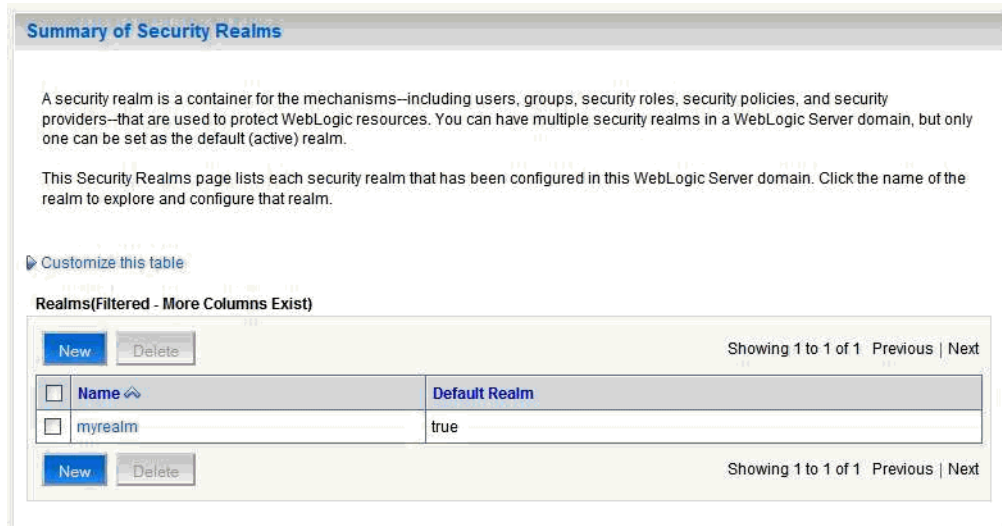
31.5.3.2 Configuring an Active Directory Authentication Provider

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 WebLogic Server Administration Console.
 For information on logging in to the WebLogic Server Administration Console, see [Section 1.13.2, "Oracle WebLogic Server Administration Console."](#)
2. From the Domain Structure pane, click **Security Realms**.
 The Summary of Security Realms pane displays (see [Figure 31–34](#)).

Figure 31–34 Summary of Security Realms Pane



3. Click your security realm.
 The Settings page for the security realm displays (see [Figure 31–35](#)).

Figure 31–35 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 Authentication subtab. The Authentication Settings pane displays (see Figure 31–36).

Figure 31–36 Authentication 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

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**.

The Create a New Authentication Provider pane displays (see [Figure 31–37](#)).

Figure 31–37 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 the authentication provider you just created in the list of providers.

The Settings page for the provider displays (see [Figure 31–38](#)).

Figure 31–38 Provider Settings Page

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 31–39](#)).

Figure 31–39 *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: 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:

SSLEnabled Specifies whether the SSL protocol should be used when connecting to the LDAP server. [More Info...](#)

Users

User Base DN: ou=WLSMEMBERS,dc= 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: {&(cn=%u)(objectclass= 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: 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 that specifies the name of the user. [More Info...](#)

User Object Class: user 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 31–3 *Active Directory Authenticator Settings*

Parameter	Value	Description
Host:		The host ID of the LDAP server

Table 31-3 (Cont.) Active Directory Authenticator Settings

Parameter	Value	Description
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	
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...

31.5.3.3 Configuring WebCenter Portal: 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 Spaces. There are two options for doing this:

- Turn off public access, by logging in to Spaces as an administrator and removing View access from the `Public-User` role. When public access is turned off, accessing the URL `http://host:port/webcenter` takes the user directly to the authenticated view rather than the default public page which has a login section. This is recommended when users are accessing Spaces only using Internet Explorer, and are confined to the domain where WNA is set up.

- If you must retain public access to Spaces, then the recommendation is to use the `oracle.webcenter.spaces.osso=true` flag when starting the `WC_Spaces` server. This flag tells 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 Spaces within the Windows network configured for WNA, or any browser is used to access Spaces from outside the Windows network domain, users see the login page after clicking the Login link.

31.5.3.4 Configuring the Discussions Server for SSO

This section describes how to configure Oracle WebCenter Portal's Discussion Server for single sign-on. Before configuring the discussions server for SSO, ensure that it has been configured to use the same identity store LDAP as Spaces, as described in [Section 29.5.1, "Migrating WebCenter Portal's Discussions Server to Use an External LDAP:"](#)

To set up the discussions server for SSO:

1. Log in to the Oracle WebCenter Portal's Discussion Server Admin Console at:

```
http://host:port/owc_discussions/admin
```

Where *host* and *port* are the host ID and port number of the `WC_Collaboration` Managed Server.

2. Open the System Properties page and edit (if it already exists) or add the `owc_discussions.sso.mode` property, setting its value to `true`.

31.6 Configuring SSO with Virtual Hosts

This section describes the OHS configuration required for an environment containing applications that use "/" as the context root, and the additional configuration required in OHS when single sign-on is involved.

This section contains the following subsections:

- [Section 31.6.1, "Understanding the Need for a Virtual Host"](#)
- [Section 31.6.2, "Configuring Virtual Hosts for OSSO"](#)
- [Section 31.6.3, "Configuring Virtual Hosts for OAM 10g"](#)
- [Section 31.6.4, "Configuring Virtual Hosts for OAM 11g"](#)
- [Section 31.6.5, "Configuring WebCenter Portal for Virtual Hosts"](#)
- [Section 31.6.6, "Testing Your Configuration"](#)

31.6.1 Understanding the Need for a Virtual Host

The WebCenter Portal Suite includes a desktop integration application that uses "/" as the context root. If this application is to be used in a single sign-on environment you need to route it through OHS. To do this without a virtual host we could add the following entry to `mod_wl_ohs.conf`:

```
<Location />
    SetHandler weblogic-handler
    WebLogicHost webcenter.example.com
    WebLogicPort 8888
```

```
</Location>
```

However, this would affect all context roots not explicitly defined, which brings us to the need for a virtual host.

The term *virtual host* refers to the practice of running more than one web site (such as `www.company1.com` and `www.company2.com`) on a single machine. Virtual hosts can be *IP-based*, meaning that you have a different IP address for each web site, or *name-based*, meaning that you have multiple names running on each IP address. The fact that they are running on the same physical server is not apparent to the end user. For more information about virtual hosts, refer to your Apache documentation.

31.6.2 Configuring Virtual Hosts for OSSO

This section describes the steps for configuring virtual hosts when OSSO is configured as the single sign-on solution. Prior to completing these steps you should already have completed the steps in [Section 31.3, "Configuring Oracle Single Sign-On \(OSSO\)."](#)

To use virtual hosts with OSSO you need to register partner applications with the virtual host option. Also, for `webtier-spaces.example.com`, you need to bypass single sign-on as some applications support only BASIC authentication and do not require single sign-on. These configurations are described in the following steps:

1. Move the `mod_osso.conf` file from `moduleconf` to the same location as `httpd.conf`. (All files in `moduleconf` are loaded automatically by default, but we need OSSO disabled for our virtual host.)
2. Update the virtual host setup in `httpd.conf` as shown in the following example:

```
NameVirtualHost *:7777

<VirtualHost *:7777>
    ServerName webtier.example.com
    include mod_osso.conf
</VirtualHost>

<VirtualHost *:7777>
    ServerName webtier-spaces.example.com
    <Location />
        SetHandler weblogic-handler
        WebLogicHost webcenter.example.com
        WebLogicPort 8888
    </Location>
    <Location /webcenter>
        Deny from all
    </Location>
    <Location /webcenterhelp>
        Deny from all
    </Location>
    <Location /rest>
        Deny from all
    </Location>
</VirtualHost>
```

By including the `mod_osso.conf` in the default virtual host we provide a single sign-on experience for the default virtual host (`webtier.example.com`), but not for the Spaces virtual host (`webtier-spaces.example.com`) as some applications do not support it.

- Restart OHS. Also remember to update the DNS with entries for `webtier-spaces.example.com`.

Note: In the `webtier-spaces.example.com` virtual host that bypasses single sign-on, only some applications need to bypass single sign-on. For other applications like Spaces, however, we need single sign-on so we deny access to these applications from this virtual host.

31.6.3 Configuring Virtual Hosts for OAM 10g

To configure OAM 10g for virtual hosts we need to bypass single sign-on for applications that only support BASIC authorization or do not require single sign-on. For more information, see "Associating a WebGate with Particular Virtual Hosts, Directories, or Files" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service for 10g*.

Prior to completing these steps you should already have completed the steps for configuring OAM 10g in [Section 31.2, "Configuring Oracle Access Manager \(OAM\)."](#)

- Locate and comment out the following configuration in `httpd.conf`:

```
#Comment out this and move to VirtualHost configuration
#<LocationMatch "/*">
#AuthType Oblix
#require valid-user
#</LocationMatch>
```

This entry causes the WebGate to intercept all requests and process them.

- Move this entry into the virtual host configuration where single sign-on is required as shown in the example below:

```
NameVirtualHost *:7777

<VirtualHost *:7777>
  ServerName webtier.example.com
  <LocationMatch "/*">
    AuthType Oblix
    require valid-user
  </LocationMatch>
</VirtualHost>

<VirtualHost *:7777>
  ServerName webtier-spaces.example.com
  <Location />
    SetHandler weblogic-handler
    WebLogicHost webcenter.example.com
    WebLogicPort 8888
  </Location>
  <Location /webcenter>
    Deny from all
  </Location>
  <Location /webcenterhelp>
    Deny from all
  </Location>
  <Location /rest>
    Deny from all
  </Location>
</VirtualHost>
```

The idea is to provide a single sign-on experience for the default virtual host (`webtier.example.com`), but not for the Spaces virtual host (`webtier-spaces.example.com`) as some applications do not support it.

- Restart OHS. Also be sure to update the DNS with entries for `webtier-spaces.example.com`.

Note: In the `webtier-spaces.example.com` virtual host that bypasses single sign-on, only some applications need to bypass single sign-on. For other applications like Spaces, however, we need single sign-on so we deny access to these applications from this virtual host.

31.6.4 Configuring Virtual Hosts for OAM 11g

To configure OAM 11g for virtual hosts we need to bypass single sign-on for applications that only support BASIC authorization or do not require single sign-on.

Prior to completing these steps you should already have completed the steps for configuring OAM 11g in [Section 31.2, "Configuring Oracle Access Manager \(OAM\)."](#)

Follow the steps below to configure virtual hosts for OAM 11g.

- Locate and comment out the following configuration in `webgate.conf`:

```
#Comment out this and move to VirtualHost configuration
#<LocationMatch "/*">
#AuthType Oblix
#require valid-user
#</LocationMatch>
```

This entry causes the WebGate to intercept all requests and process it.

- Move this entry into the virtual host configuration in `httpd.conf` where single sign-on is required, as shown in the example below:

```
NameVirtualHost *:7777

<VirtualHost *:7777>
  ServerName webtier.example.com
  <LocationMatch "/*">
    AuthType Oblix
    require valid-user
  </LocationMatch>
</VirtualHost>

<VirtualHost *:7777>
  ServerName webtier-spaces.example.com
  <Location />
    SetHandler weblogic-handler
    WebLogicHost webcenter.example.com
    WebLogicPort 8888
  </Location>
  <Location /webcenter>
    Deny from all
  </Location>
  <Location /webcenterhelp>
    Deny from all
  </Location>
  <Location /rest>
    Deny from all
  </Location>
```

```
</VirtualHost>
```

The idea is to provide a single sign-on experience for the default virtual host (`webtier.example.com`), but not for the Spaces virtual host (`webtier-spaces.example.com`) as some applications do not support it.

3. Restart OHS. Also be sure to update the DNS with entries for `webtier-spaces.example.com`.

Note: In the `webtier-spaces.example.com` virtual host that bypasses single sign-on, only some applications need to bypass single sign-on. For other applications like Spaces, however, we need single sign-on so we deny access to these applications from this virtual host.

31.6.5 Configuring WebCenter Portal for Virtual Hosts

This section describes the additional configurations required for applications routed through the virtual host.

Sharepoint

Typically when you use the "Edit with Word" or similar features for MS Office products, the WebCenter Portal Sharepoint application obtains the host name and port name from the current request. However, in this case the Sharepoint application needs to be routed through the virtual host requiring that some system properties be set in `setDomainEnv` in the WebLogic domain. For a cluster setup, be sure to change these properties on every machine.

```
-Dnon_sso_host=webtier-spaces.example.com
-Dsso_base_url=http://webtier.example.com:7777
```

31.6.6 Testing Your Configuration

This section describes how you can test your virtual host and single sign-on configuration.

Sharepoint

1. Access `http://webtier.example.com:7777/webcenter` and check that you are challenged by SSO.
2. Log in and choose an MS Word document and click **Edit with Word**. Click **OK** when you see a confirmation dialog. Word should challenge you for BASIC authentication. Enter your credentials and you should be able to see the document
3. Navigate to **Office icon > Server > Document Management Information** and click **Open Site in Browser**. This should open the space to which the document belongs in your default browser.

Note that you will be prompted with a BASIC authentication challenge as MS Office integration has a restriction where it needs to go to the same URL as the one for the document. You will then be redirected to the space through `webtier.example.com` and be prompted for to login if not already logged in..

Configuring Framework Applications for Single Sign-on

This chapter describes how to configure WebCenter Portal: Framework applications for single sign-on (SSO). All of the configurations described in this chapter assume that you have already configured SSO as described in [Section 31, "Configuring Single Sign-on."](#)

This chapter includes the following sections:

- [Section 32.1, "Configuration Overview"](#)
- [Section 32.2, "Single Sign-on Prerequisites"](#)
- [Section 32.3, "Configuring the WebTier"](#)
- [Section 32.4, "Configuring Framework and Portlet Producer Applications for OAM"](#)
- [Section 32.5, "Configuring Framework Applications for OSSO"](#)
- [Section 32.6, "Configuring Framework Applications for SAML SSO"](#)

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."](#)

32.1 Configuration Overview

Oracle WebCenter Portal supports single sign-on (SSO) for the following SSO solutions for WebCenter Portal: Framework applications:

- OAM 10g
- OAM 11g
- OSSO
- SAML SSO (Framework application as a destination application)
- SAML SSO (Framework application as the source application)

Before a Framework application can participate in single sign-on, in addition to the SSO configuration described in [Chapter 31, "Configuring Single Sign-on,"](#) you must also configure the Framework application itself for the chosen SSO solution. To do this, follow the instructions in [Chapter 32.2, "Single Sign-on Prerequisites,"](#) and then

continue with the steps for your particular solution. The only exception to this is for SAML SSO, where the Framework application is acting as the source application where all the steps, including the prerequisites, are covered in [Section 32.6.2, "Configuring SAML SSO for a Source Framework Application."](#)

32.2 Single Sign-on Prerequisites

All Framework applications participating in SSO need to have certain common configurations in place regardless of the single sign-on solution used to protect the application. The only exception to this is for SAML SSO where the Framework application is acting as the source application (see [Section 32.6.2, "Configuring SAML SSO for a Source Framework Application"](#) for more information).

The common single sign-on prerequisites are covered in the following subsections:

- [Section 32.2.1, "Adding CLIENT-CERT in web.xml"](#)
- [Section 32.2.2, "Setting the Cookie Path for JSESSIONID"](#)
- [Section 32.2.3, "Determining the Public and Protected URIs for Your Application"](#)
- [Section 32.2.4, "Implications of Embedded Login"](#)
- [Section 32.2.5, "Handling Logout"](#)

32.2.1 Adding CLIENT-CERT in web.xml

All SSO solutions use an identity asserter configured on the WLS domain that asserts the type of assertion that an SSO configuration provides. For example, for OAM, it asserts based on the `ObSSOCookie` or `OAM_REMOTE_USER` header; for SAML SSO it asserts a SAML assertion.

For an asserter to assert identity, the application must specify `CLIENT-CERT` as its authentication method in its login configuration. Consequently, your application's `web.xml` file must have `CLIENT-CERT` specified as the `auth-method` as shown in the following example:

```
<login-config>
  <auth-method>CLIENT-CERT, FORM</auth-method>
```

Note that in Weblogic, you can specify comma-separated authentication methods. In this example, if the SSO assertion is not available (`CLIENT-CERT`), then the application will fall back to `FORM`-based authentication.

32.2.2 Setting the Cookie Path for JSESSIONID

For SSO setups, Oracle recommends that you set an application cookie path. You can do this in WLS by editing the `weblogic.xml` file and adding the following entry:

```
<session-descriptor>
  <cookie-path>/customportal</cookie-path>
</session-descriptor>
```

where `customportal` is the context root of your application.

32.2.3 Determining the Public and Protected URIs for Your Application

An SSO configuration involves specifying the public and protected URIs of your application. Some SSO solutions, like OSSO and SAML SSO, require only the

protected URIs to be specified. The following list shows the typical protected and public URIs for a Framework application:

Public URI:

```
/<app-context-root>
```

Protected URI:

```
/<app-context-root>/adfAuthentication
```

You can determine the protected URIs for your application by checking the `security-constraint` node of the `web.xml` file as shown in the following example:

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>adfAuthentication</web-resource-name>
    <url-pattern>/adfAuthentication</url-pattern>
  </web-resource-collection>
  <auth-constraint>
    <role-name>valid-users</role-name>
  </auth-constraint>
</security-constraint>
```

Note that the entries in the `security-constraint` node are always relative to the application context root. In this example, this security constraint translates to `/app-context-root/adfAuthentication`. If there were another security constraint specified, `/admin` for example, then that would translate to `/app-context-root/admin`.

32.2.4 Implications of Embedded Login

Framework applications typically use a form-based login mechanism where a login page is configured in the `login-config` section of the `web.xml` configuration file (note that there is no separate login configuration file). Applications can also embed a login area in the page template, or a provide landing page. This usually submits the users credentials to `j_security_check` for authentication. For SSO, however, authentication must be done through an SSO login challenge.

32.2.5 Handling Logout

The ADF Authentication Servlet is equipped to handle logout for all SSO solutions, and your application's logout should invoke the ADF Authentication Servlet for logout. To do this, modify the navigation rule for successful logout in your application's `faces-config.xml` file as shown in the example below:

```
<navigation-case>
  <from-outcome>logout_success</from-outcome>
  <to-view-id>/adfAuthentication?logout=true&end_url=/</to-view-id>
  <redirect/>
</navigation-case>
```

The `end_url` parameter for `/adfAuthentication` can be any URL that you want to direct the user to after a successful logout. For example, specifying `/` would take the user to the application's default page.

32.3 Configuring the WebTier

If your environment has a WebTier front-ending your enterprise applications you'll need to configure it for SSO. The WebTier is required for OAM and OSSO solutions, and is used in a SAML SSO solution when Content Server is involved.

1. Add a mapping for your application in `mod_wl_ohs.conf` as shown in the example below:

```
<Location /customportal>
    SetHandler weblogic-handler
    WebLogicHost webcenter.example.com
    WebLogicPort 8888
</Location>
```

where `customportal` is the context root of your application.

2. Restart the Oracle HTTP Server.

32.4 Configuring Framework and Portlet Producer Applications for OAM

This section describes how to configure your WebCenter Portal: Framework or WebCenter Portal: Portlet Producer application for OAM 10g and 11g. Prior to following the steps in this section you should already have followed the instructions in [Section 31.2, "Configuring Oracle Access Manager \(OAM\)"](#) to set up SSO for Spaces and related applications. You should also have completed the configurations in [Section 32.2, "Single Sign-on Prerequisites."](#)

Note: Prior to starting, you should already have configured the required OAM Asserter and Authenticator pointing to the identity store LDAP used by OAM in the domain where your Framework application is deployed. If you have not done this, follow the instructions in [Section 31.2, "Configuring Oracle Access Manager \(OAM\)"](#) before starting.

This section includes the following subsections:

- [Section 32.4.1, "Configuring Framework Applications for OAM 10g"](#)
- [Section 32.4.2, "Configuring Portlet Producer Applications for OAM 10g"](#)
- [Section 32.4.3, "Configuring Framework Applications for OAM 11g"](#)
- [Section 32.4.3, "Configuring Framework Applications for OAM 11g"](#)

32.4.1 Configuring Framework Applications for OAM 10g

This section describes how to configure a Framework application for single sign-on using OAM 10g. Prior to configuring your application you should already have completed the OAM installation and configuration as described in [Section 31.2, "Configuring Oracle Access Manager \(OAM\)."](#)

To configure a Framework application for OAM 10g:

1. Log in to the OAM Console using your browser to navigate to:
`http://host:port/access/oblix`
2. Click **Policy Manager**.

3. Locate the policy domain that you created to protect your WebCenter Portal resources.
4. Open the Resources tab and click **Add**.
5. Add the resources. For each resource:
 - a. Select `HTTP` as the **Resource Type**.
 - b. Select the **Host Identifier** for the WebCenter Portal Web Tier.
 - c. Enter the **URL Prefix** (`/<app-context-root>`) for the application.
 - d. Enter a **Description** for the resource.
 - e. Make sure that **Update Cache** is selected, and then click **Save**.
6. Repeat step 5 to add `/<app-context-root>/adfAuthentication` as a resource.
7. Go to the Policies tab and locate the public policy.
8. Open the policy and select the resource created in step 5 (i.e., `/<app-context-root>`).
9. Save your changes.
10. Restart the WebTier and test your changes.

32.4.2 Configuring Portlet Producer Applications for OAM 10g

This section describes how to configure Portlet Producer applications for single sign-on using OAM 10g. Prior to configuring your Portlet Producer application follow the steps in [Section 32.4.1, "Configuring Framework Applications for OAM 10g,"](#) then complete the steps below.

To configure a Portlet Producer application for OAM 10g:

1. Log in to the OAM Console using your browser to navigate to:
`http://host:port/access/oblix`
2. Click **Policy Manager**.
3. Locate the policy domain that you created to protect your WebCenter Portal resources.
4. Open the Resources tab and click **Add**.
5. Select `HTTP` as the **Resource Type**.
6. Select the **Host Identifier** for the WebCenter Portal WebTier.
7. Enter the **URL Prefix** (`/<app-context-root>/portlets`) for the application.
8. Enter a **Description** for the resource.
9. Make sure that **Update Cache** is selected, and then click **Save**.
10. Go to the Policies tab and locate the Exclusion Scheme policy and select the newly created Portlet Producer resource for this policy.
11. Open the policy and select the resource created in step 5 (i.e., `/<app-context-root>/portlets`).
12. Save your changes.
13. Restart the WebTier and test your changes.

32.4.3 Configuring Framework Applications for OAM 11g

This section describes how to configure a Framework application for single sign-on using OAM 11g. Prior to configuring your application you should already have completed the OAM installation and configuration as described in [Section 31.2, "Configuring Oracle Access Manager \(OAM\)."](#)

To configure a Framework application for OAM 11g:

1. Log in to the OAM Console using your browser to navigate to:
`http://host:port/oamconsole`
2. Go to **Policy Configuration > Application Domains**.
The Policy Manager pane displays.
3. Locate the application domain you created using the name used when registering the WebGate agent.
4. Open the Resources tab and click **New Resource**.
5. Add the resources for the Framework application. For each resource:
 - a. Select HTTP as the **Resource Type**.
 - b. Select the **Host Identifier** created while registering the WebGate agent.
 - c. Enter the **Resource URL** (`/<app-context-root>*`) for the application.
 - d. Enter a **Description** for the resource.
 - e. Set the **Protection Level** to Unprotected.
 - f. Set the **Authentication Policy** to Public Resource Policy.
 - g. Set the **Authorization Policy** to Protected Resource Policy.
 - h. Click **Apply**.
6. Repeat step 5 to add `/<app-context-root>/.../*` as a resource.
7. Add `/<app-context-root>/adfAuthentication*` as a resource:
 - a. Select HTTP as the **Resource Type**.
 - b. Select the **Host Identifier** created while registering the WebGate agent.
 - c. Enter the **Resource URL** (`/<app-context-root>/adfAuthentication*`) for the application.
 - d. Enter a **Description** for the resource.
 - e. Set the **Protection Level** to Protected.
 - f. Set the **Authentication Policy** to Protected Resource Policy.
 - g. Set the **Authorization Policy** to Protected Resource Policy.
 - h. Click **Apply**.
8. Restart the WebTier and test your changes.

32.4.4 Configuring Portlet Producer Applications for OAM 11g

This section describes how to configure Portlet Producer applications for single sign-on using OAM 11g. Prior to configuring your Portlet Producer application follow the steps in [Section 32.4.3, "Configuring Framework Applications for OAM 11g,"](#) then complete the steps below.

To configure a Portlet Producer application for OAM 11g:

1. Log in to the OAM Console using your browser to navigate to:
`http://host:port/access/oblix`
2. Click **Policy Manager**.
3. Locate the policy domain that you created to protect your WebCenter Portal resources.
4. Open the Resources tab and click **Add**.
5. Select HTTP as the **Resource Type**.
6. Select the **Host Identifier** created while registering the WebGate agent.
7. Enter the **URL Prefix** (`/<app-contextroot>/portlets/.../*`) for the application.
8. Enter a **Description** for the resource.
9. Set the **Protection Level** to `Excluded`, and then click **Save**.
10. Restart the WebTier and test your changes.

32.5 Configuring Framework Applications for OSSO

This section describes how to configure your WebCenter Portal: Framework application for OSSO. Prior to following the steps in this section you should already have followed the instructions in [Section 31.3, "Configuring Oracle Single Sign-On \(OSSO\)"](#) to set up SSO for Spaces and related applications. You should also have completed the configurations in [Section 32.2, "Single Sign-on Prerequisites."](#)

Note: Prior to starting, you should already have configured the required OSSO Asserter and Authenticator pointing to the identity store (OID) used by OSSO in the domain where your Framework application is deployed. If you have not done this, follow the instructions [Section 31.3, "Configuring Oracle Single Sign-On \(OSSO\)"](#) before starting.

To configure a Framework application for OSSO:

1. Locate and open the `mod_osso.conf` file in OHS.
2. Add the following entry for your Framework application to the other similar entries:

```
<Location /<app-context-root>/adfAuthentication>
    OsoSendCacheHeaders off
    require valid-user
    AuthType Oso
</Location>
```

3. Restart OHS.

32.6 Configuring Framework Applications for SAML SSO

This section describes how to set up SAML SSO for Framework applications. Note that SAML single sign-on is only recommended for smaller environments (a department, for example) where no enterprise SSO solution is available.

The steps are divided into two scenarios:

- **Scenario 1: A Framework application as a destination application**

This is the default SAML SSO behaviour provided by the WebCenter Portal SAML SSO scripts, where the Spaces application is the source application and all other applications are destination applications (that is, you need to be logged into Spaces for single sign-on with other destination applications to work).

- **Scenario 2: A Framework application as a source application**

This behaviour is not supported by the WebCenter Portal SAML SSO scripts and requires manual configuration. In this instance you want your Framework application to act as the SAML source, and other applications (including Spaces) to act as destination applications (that is, your Framework application is the first point of access and you need to be logged into it for single sign-on with other destination applications to work).

These two approaches to configuring SAML for Framework applications is described in the following subsections:

- [Section 32.6.1, "Configuring SAML SSO for a Destination Framework Application"](#)
- [Section 32.6.2, "Configuring SAML SSO for a Source Framework Application"](#)

32.6.1 Configuring SAML SSO for a Destination Framework Application

Prior to following the steps in this section, you should already have completed the prerequisites and steps in [Section 31.4, "Configuring SAML-based Single Sign-on"](#) that describe how to set up SSO for Spaces and related applications. The steps in this section supplement that setup with configuration steps for your Framework application.

In this scenario, the Spaces application continues to act as the source application with your new Framework application participating in single sign-on as a destination application (that is, if you are logged into Spaces, when you access one of your Framework application's protected URIs, you are automatically logged in). If you are not already logged into Spaces and you access a protected URI, you will be directed to the Spaces login page and then redirected back to your application's secure page.

The steps below assume that:

- Your Framework application is deployed in the Spaces domain where the `configureSpaces.py` script was run. If your Framework application is in a different domain, then you'll need to create a `SAMLIdentityAsserterV2` ID Asserter in the WLS Administration console (**security realm > providers > authenticator**) and restart WLS. You then need to export the certificate used in your SAML SSO setup and register it under the SAML identity asserter you created.
- The steps and example parameter values below assume you are using the `demoidentity` certificate. If you are using a different certificate, change the certificate name where appropriate.
- If a WebTier is part of the configuration, the host and port IDs are those of the WebTier host and WebTier port.

This section includes the following subsections:

- [Section 32.6.1.1, "Enabling the Destination Site"](#)
- [Section 32.6.1.2, "Configuring a Relying Party"](#)

- [Section 32.6.1.3, "Configuring an Asserting Party"](#)

32.6.1.1 Enabling the Destination Site

To enable the destination site for your Framework application:

1. Log onto the WLS Administration Console for the Spaces domain.
2. Select **Servers > [ServerHostingPortalApp] > Configuration > Federation Services > SAML 1.1 Destination Site**.
3. Enter the parameters for the destination site as shown in [Table 32–1](#):

Table 32–1 Destination Site Parameters

Parameter	Value	Description
Destination Site Enabled	Selected	Specifies whether the destination site is enabled.
ACS Requires SSL	Unselected	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	<code></app-context-root>/samlacs/acs</code> (add on top, leave the rest as is)	The Assertion Consumer URIs. In this case, we have chosen for the ACS to reside within the target application so that it uses the same login cookie.
POST Recipient Check Enabled	Selected	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	Selected	Specifies whether the POST one-use check is enabled.

4. Save your changes, leaving the rest as their default values.
5. Restart the server hosting the Framework application.

32.6.1.2 Configuring a Relying Party

To configure a relying party for your Framework application:

1. Log onto the WLS Administration Console for the Spaces domain.
2. Select **Security Realms > Providers > Credential Mapping > wcsamlcm > Management > Relying Parties**.
3. Create a new relying party using the the parameters in [Table 32–2](#):

Table 32–2 Relying Party Parameters

Parameter	Value	Description
Profile	Browser/POST	The SAML profile used by this SAML Relying Party.
Enabled	Selected	The state of this SAML Relying Party.
Description	Framework application	A short description of this Relying Party

Table 32–2 (Cont.) Relying Party Parameters

Parameter	Value	Description
Target URL	http://host:port/<app-context-root>	The destination site URL for which authentication is requested.
Assertion Consumer URL	http://host:port/<app-context-root>/samlacs/acs	The URL at which an Assertion Consumer Service for this SAML Relying Party can be reached. Indicates the URL to which an assertion or artifact should be POSTed or redirected. Note: If you have checked ACS requires SSL while configuring destination site federation services, then use https protocol and the SSL port for the managed server
Assertion Consumer Properties	APID=ap_0000X	The X points to ID of the asserting party you will create in next step.
Sign Assertions	Selected	Specifies whether generated assertions for this SAML Relying Party are signed.
Include KeyInfo	Selected	Indicates whether a <ds:keyinfo> element containing the signing certificate should be included when signing assertions. Default value is true. This value is ignored if Sign Assertions is false.

4. Save your changes, leaving the rest as their default values.

32.6.1.3 Configuring an Asserting Party

To configure an asserting party for your Framework application:

1. Log onto the WLS Administration Console for the Spaces domain.
2. Select **Security Realms > Providers > Authentication > wcsamlia > Management > Asserting Parties**.
3. Create a new asserting party using the the parameters in [Table 32–3](#):

Table 32–3 Asserting Party Parameters

Parameter	Value	Description
Profile	Browser/POST	The SAML profile used with this partner.
Enabled	Selected	Specifies whether this Asserting Party can be used to obtain SAML assertions
Description	Spaces	A short description of this Asserting Party
Target URL	http://host:port/w ebcenter	The target URL of this SAML asserting party.
POST Signing Certificate alias	demoidentity	The alias of the certificate trusted for verifying signatures on SAML protocol elements from this asserting party. Must be set for Browser/POST profile.

Table 32–3 (Cont.) Asserting Party Parameters

Parameter	Value	Description
Source Site Redirect URIs	<code></app-context-root>/adfAuthentication</code>	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. Note: Due to this setting, when you access the destination site first, you are redirected to the ITS url configured which in this case is within the source app, your session is established source app and then redirected to the destination site.
Source Site ITS URL	<code>http://host:port/webcenter/samlits/its</code>	The Intersite Transfer Service (ITS) URL of the SAML Source Site for this asserting party. Use this with SSO profiles only, to support the destination site as the first access point scenario, whereby a user trying to access a destination site URL prior to being authenticated 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. Note: If you check ITS requires SSL in Source Site Federation Services, then you need to change Source Site ITS URL to use HTTPS and the server's SSL port.
Source Site ITS parameters	<code>RPID=rp_0000x</code>	Replace the x with the ID of the relying party you created previously.
Issuer URI	<code>http://www.oracle.com/webcenter</code>	The issuer URI of the SAML Authority issuing assertions for this SAML asserting party.
Signature Required	Selected	If true, assertions must be signed. If false, signature elements are not required, but will be verified if present.
Assertion Signing Certificate alias	<code>demoidentity</code>	

4. Save your changes, leaving the rest as their default values.
5. Continue by testing that single sign-on works as expected.

32.6.2 Configuring SAML SSO for a Source Framework Application

In this scenario the Framework application acts as the source application and other applications (like Spaces) are the destinations. For configurations that include Content Server, prior to completing the configurations in this section you should have followed the relevant steps in [Section 31.4.2.1.1, "Configuring Oracle Content Server for SAML SSO."](#)

The steps below are based on the following assumptions:

- The WebCenter Portal SAML SSO scripts have not been run. The scripts configure Spaces to act as the source application, so these steps should be done manually.
- You are using the default `demoidentity` certificate and you have already exported the certificate from the domain hosting your Framework application into `demoidentity.der`.
- Your Framework application is `/customportal`.
- For configurations that include Content Server and if a WebTier is part of the configuration, the host and port IDs are those of the WebTier host and WebTier port.

This section contains the following subsections:

- [Section 32.6.2.1, "Protecting SAML ITS"](#)
- [Section 32.6.2.2, "Setting the Cookie Path for JSESSIONID"](#)
- [Section 32.6.2.3, "Setting the SSO Property to True"](#)
- [Section 32.6.2.4, "Configuring the SAML Credential Mapping Provider"](#)
- [Section 32.6.2.5, "Configuring a Relying Party"](#)
- [Section 32.6.2.6, "Configuring the Source Site Federation Services"](#)
- [Section 32.6.2.7, "Configuring the SAML Identity Assertion Provider"](#)
- [Section 32.6.2.8, "Configuring the Destination Site Federation Services"](#)
- [Section 32.6.2.9, "Configuring Other Destination Applications"](#)

32.6.2.1 Protecting SAML ITS

In the `web.xml` file of your Framework application, add the following entry after the entry for protecting `/adfAuthentication`:

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>samlits</web-resource-name>
    <url-pattern>/samlits/its</url-pattern>
  </web-resource-collection>
  <auth-constraint>
    <role-name>valid-users</role-name>
  </auth-constraint>
</security-constraint>
```

32.6.2.2 Setting the Cookie Path for JSESSIONID

For SSO setups, Oracle recommends that you set a cookie path to the context root of your application. You can do this in WLS by editing the `weblogic.xml` file and adding the following entry:

```
<session-descriptor>
  <cookie-path>/customportal</cookie-path>
</session-descriptor>
```

where `customportal` is the context root of your application.

32.6.2.3 Setting the SSO Property to True

Since the Spaces application now acts as a destination application, you need to hide the login area on the Spaces landing page. To do this, set the following property in

your `setDomainEnv` file and restart the `WC_Spaces` server for the changes to take effect.

```
EXTRA_JAVA_PROPERTIES="-Doracle.webcenter.spaces.osso=true
${EXTRA_JAVA_PROPERTIES}"
export EXTRA_JAVA_PROPERTIES
```

32.6.2.4 Configuring the SAML Credential Mapping Provider

In the security realm of the domain hosting your Framework application, create a SAML Credential Provider V2 (`SAMLCredentialMapperV2`) instance. Note that the SAML Credential Mapping provider is not part of the default security realm. Configure the SAML Credential Mapping provider as a SAML authority, using the **Issuer URI**, **Name Qualifier**, and other attributes as shown in [Table 32-4](#):

Table 32-4 SAML Credential Mapping Provider Parameters

Parameter	Value	Description
Issuer URI	<code>http://www.oracle.com/webcenter</code>	The Issuer URI (name) of this SAML Authority. This unique URI tells the destination site (<code>owc_wiki</code>) the origin of the SAML message and allows it to match it with the key. Typically, the URL is used to guarantee uniqueness.
Name Qualifier	<code>oracle.com</code>	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 collisions.
Signing Key Alias	<code>demoidentity</code>	The alias used to retrieve from the keystore the key that is used to sign assertions.
Signing Key Passphrase	<code>DemoIdentityPassPhrase</code>	The credential (password) used to retrieve from the keystore the keys used to sign assertions.

Save your changes, accepting the defaults for the rest of the parameters, and restart all of WLS.

32.6.2.5 Configuring a Relying Party

You'll need to configure relying parties for each of the destination applications. The steps below show you how to do using Spaces as an example. For other applications, refer to [Table 32-10](#) in [Section 32.6.2.9, "Configuring Other Destination Applications,"](#) and modify the highlighted values appropriately using the steps below as a reference.

To configure a relying party for Spaces:

1. Log onto the WLS Administration Console for the Spaces domain.
2. Select **Security Realms > RealmName > Providers > Credential Mapping > SAMLCredentialMapperName > Management > Relying Parties**.
3. Create a new relying party using the the parameters in [Table 32-5](#):

Table 32–5 Spaces Parameters for Relying Party

Parameter	Value	Description
Profile	Browser/POST	The SAML profile used by this SAML Relying Party.
Enabled	Selected	The state of this SAML Relying Party.
Description	Spaces	A short description of this Relying Party
Target URL	http://host:port/w ebcenter	The destination site URL for which authentication is requested.
Assertion Consumer URL	http://host:port/w ebcenter/samlacs/a cs	The URL at which an Assertion Consumer Service for this SAML Relying Party can be reached. Indicates the URL to which an assertion or artifact should be POSTed or redirected. Note: If you have checked ACS requires SSL while configuring destination site federation services, then use https protocol and the SSL port for the 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. For a 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 for your Framework application (customportal), which we will configure later in the SAML Identity Asserter of the domain hosting the Framework application, and which provides the source site and ITS details.
Sign Assertions	Selected	Specifies whether generated assertions for this SAML Relying Party are signed.
Include KeyInfo	Selected	Indicates whether a <ds:keyinfo> element containing the signing certificate should be included when signing assertions. Default value is true. This value is ignored if Sign Assertions is false.

4. Save your changes, leaving the rest as their default values.

32.6.2.6 Configuring the Source Site Federation Services

To configure the source site Federation:

1. Log onto the WLS Administration Console for the Spaces domain.
2. Select **Environment > Servers > ServerHostingCustomPortal > Configuration > Federation Services > SAML 1.1 Source Site**.

3. Configure the SAML source site attributes as shown in [Table 32–6](#).

Table 32–6 Source Site Federation Services Parameters

Parameter	Value	Description
Source Site Enabled	Selected	Allow the WebLogic server instance to serve as a SAML source site by setting Source Site Enabled to true.
Source Site URL	<code>http://host:port/customportal</code>	Set the URL for the SAML source site. 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	demoidentity	The SAML source site requires a trusted certificate with which to sign assertions. Add this certificate to the keystore and enter the credentials (alias and passphrase) 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	DemoIdentityPassPhrase	The SAML source site requires a trusted certificate with which to sign assertions. Add this certificate to the keystore and enter the credentials (alias and passphrase) 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>/customportal/samlits/its</code> (Add on top, leave the rest as is.)	Specify the URIs for the Intersite Transfer Service and (to support Browser/Artifact profile) the Assertion Retrieval Service. These URIs are also specified in the configuration of an Asserting Party.
Assertion Retrieval URIs	<code>/customportal/samars/ars</code> (Add on top, leave the rest as is.)	Applicable only when Artifact profile is used for REST.
ITS Requires SSL	Deselected	If you select this, then you need to change the Source Site ITS URL specified in the SAML Asserting party configuration in SAML Identity provider as HTTPS and the server's SSL port.
ARS Requires SSL	Deselected	Applicable only when Artifact profile is used

4. Save your changes, leaving the rest at their default values.
5. Restart the server hosting the Framework application.

32.6.2.7 Configuring the SAML Identity Assertion Provider

To configure the SAML identity assertion provider:

1. Log onto the WLS Administration Console for the Spaces domain.
2. Create a SAML Identity Assertion Provider V2 instance as described in [Section 32.6.1.3, "Configuring an Asserting Party,"](#) restarting all of WLS after saving your changes.
3. Log back onto the WLS Administration Console and go to **Security Realms > RealmName > Providers > Authentication > *SAMLIdentityAsserterName* > Management > Certificates.**
4. Configure a certificate for the SAML identity asserter:
5. Configure a certificate for the SAML identity asserter using the values shown in [Table 32-7.](#)

Table 32-7 Identity Asserter Certificate Parameters

Parameter	Value	Description
alias	demoidentity	Name you would you like to assign to your new certificate.
Path	WEBLOGIC_HOME/server/lib/demoidentity.der	Specify the path name of a .pem or .der file containing the X509 certificate you wish to import.

6. Go to **Security Realms > RealmName > Providers > Authentication > *SAMLIdentityAsserterName* > Management > Asserting Parties.**
7. Create a new asserting party using the the parameters in [Table 32-8.](#) Use the same profile you chose for the corresponding relying party in [Section 32.6.2.5, "Configuring a Relying Party."](#)

Table 32-8 Asserting Parties Parameters

Parameter	Value	Description
Profile	Browser/POST	The SAML profile used with this partner.
Enabled	Selected	Specifies whether this Asserting Party can be used to obtain SAML assertions
Description	Framework application for Spaces	A short description of this Asserting Party
Target URL	http://host:port/customportal	The target URL of this SAML asserting party.
POST Signing Certificate alias	demoidentity	The alias of the certificate trusted for verifying signatures on SAML protocol elements from this asserting party. Must be set for Browser/POST profile.

Table 32–8 (Cont.) Asserting Parties Parameters

Parameter	Value	Description
Source Site Redirect URIs	/webcenter/adfAuthentication	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. Note: This setting, when you access the destination site first, redirects you to the ITS URL configured (which in this case is within the source application), your session is established for the source application, and you are then redirected to the destination site.
Source Site ITS URL	http://host:port/customportal/samlits/its T	The Intersite Transfer Service (ITS) URL of the SAML Source Site for this asserting party. Use this with SSO profiles only, to support the destination site as the first access point scenario, whereby a user trying to access a destination site URL prior to being authenticated 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. Note: If you check ITS requires SSL in Source Site Federation Services, then you need to change 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 Spaces as specified in the SAML Credential Mapping provider of the WLS domain for the Framework application that provides the destination site details.
Issuer URI	http://www.oracle.com/webcenter	The issuer URI of the SAML Authority issuing assertions for this SAML asserting party.
Signature Required	Selected	If true, assertions must be signed. If false, signature elements are not required, but will be verified if present.
Assertion Signing Certificate alias	demoidentity	The alias of the certificate trusted for verifying signatures on assertions from this Asserting Party. This must be set if Signature Required is true. The certificate must also be registered in the SAML Identity Asserter's certificate registry.

8. Save your changes, leaving the rest at their default values.

32.6.2.8 Configuring the Destination Site Federation Services

To configure the destination site federation services:

1. From the WLS Administration Console, go to **WC Domain > WC_Spaces > Configuration > Federation Services > SAML 1.1 Destination Site [Spaces]**
2. Configure the SAML destination site attributes using the values in [Table 32–9](#).

Table 32–9 Destination Site Parameters

Parameter	Value	Description
Destination Site Enabled	Selected	Specifies whether the Destination Site is enabled.
ACS Requires SSL	Deselected	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 the target server's SSL port.
Assertion Consumer URIs	/webcenter/samlacs /acs /rss/samlacs/acs /rest/samlacs/acs (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 application so that it uses the same login cookie.
POST Recipient Check Enabled	Selected	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	Selected	Specifies whether the POST one-use check is enabled.

3. Save your changes, leaving the rest at their default values.
4. Restart the Spaces server.

32.6.2.9 Configuring Other Destination Applications

If you want applications other than Spaces to act as destination applications for your Framework application, then perform the following steps:

1. Ensure you have the SAML ID asserter and certificate registered in each domain that hosts destination applications (refer to steps 1 - 5 of section [Section 32.6.2.7, "Configuring the SAML Identity Assertion Provider"](#)).
2. Create a relying party for your destination application in the WLS domain hosting your Framework application as you did for Spaces in [Section 32.6.2.5, "Configuring a Relying Party."](#) See [Table 32–10](#) for appropriate values for each application.
3. In your destination application's WLS domain, create a corresponding asserting party similar to what you did for Spaces. Use the steps for creating an asserting party in [Section 32.6.2.7, "Configuring the SAML Identity Assertion Provider."](#) Be sure to set the source redirect URI appropriately to the secure URI for your destination application. See [Table 32–10](#) for appropriate values for each application.

4. Ensure your asserting and relying parties are enabled and point to each other appropriately. That is, the Source Site ITS parameters in the asserting party and the Assertion Consumer Properties in the relying party point to each other appropriately.
5. Ensure you have enabled destination site federation services for the server hosting your destination application, and have added entries for `/yourdestinationapp/samlacs/acs` similar to what you did for the WC_Spaces server in as you did in [Section 32.6.2.8, "Configuring the Destination Site Federation Services."](#) See [Table 32–10](#) for appropriate values for each application.

Table 32–10 Settings for Destination Applications Other than Spaces

Destination Application	Target URL (Relying Party)	ACS URL (Relying Party)	ACS URI (DestinationSiteFederationServices)	Source Redirect URI (Asserting Party)
RSS	<code>http://host:port/rss</code>	<code>http://host:port/rss/samlacs/acs</code>	<code>/rss/samlacs/acs</code>	<code>/rss/rssservlet</code>
REST	<code>http://host:port/rest</code>	<code>http://host:port/rest/samlacs/acs</code>	<code>/rest/samlacs/acs</code>	<code>/rest/api/resourceIndex</code>
Discussions	<code>http://host:port/owc_discussions</code>	<code>http://host:port/owc_discussions/samlacs/acs</code>	<code>/owc_discussions/samlacs/acs</code>	<code>/owc_discussions/admin/forum-main.jsp</code> <code>/owc_discussions/admin/content-main.jsp</code> <code>/owc_discussions/login!withRedirect.jspa</code> <code>/owc_discussions/login!default.jspa</code> <code>/owc_discussions/login.jspa</code>
ActivityGraph Engines	<code>http://host:port/activitygraph-engines</code>	<code>http://host:port/activitygraph-engines/samlacs/acs</code>	<code>/activitygraph-engines/samlacs/acs</code>	<code>/activitygraph-engines/index.jsp</code>
Content Server	<code>http://host:port</code>	<code>http://host:port/samlacs/acs</code>	<code>/samlacs/acs</code>	<code>/adfAuthentication</code>
Worklist Detail	<code>http://host:port/workflow/WebCenterWorklistDetail</code>	<code>http://host:port/workflow/WebCenterWorklistDetail/samlacs/acs</code>	<code>/WebCenterWorklistDetail/samlacs/acs</code>	<code>/workflow/WebCenterWorklistDetail/faces/adf.task-flow</code>
Worklist SDP	<code>http://host:port/workflow/sdpmessagingsca-ui-worklist</code>	<code>http://host:port/workflow/sdpmessagingsca-ui-worklist/samlacs/acs</code>	<code>/sdpmessagingsca-ui-worklist/samlacs/acs</code>	<code>/workflow/sdpmessagingsca-ui-worklist/faces/adf.task-flow</code>
Worklist Integration	<code>http://host:port/integration/worklistapp</code>	<code>http://host:port/integration/worklistapp/samlacs/acs</code>	<code>/worklistapp/samlacs/acs</code>	<code>/integration/worklistapp/ssologin</code> <code>/integration/worklistapp/faces/home.jspx</code>

Configuring SSL

This chapter describes how to secure WebCenter Portal applications (including Framework applications and Spaces) and components with SSL.

This chapter includes the following sections:

- [Section 33.1, "Securing the Browser Connection to Spaces with SSL"](#)
- [Section 33.2, "Securing the Browser Connection to a Framework Application with SSL"](#)
- [Section 33.3, "Securing the Connection from Oracle HTTP Server to Spaces with SSL"](#)
- [Section 33.4, "Securing the Browser Connection to the Discussions Service with SSL"](#)
- [Section 33.5, "Securing the Spaces Connection to Portlet Producers with SSL"](#)
- [Section 33.6, "Securing the Spaces Connection to the LDAP Identity Store"](#)
- [Section 33.7, "Securing the Spaces Connection to Content Server with SSL"](#)
- [Section 33.8, "Securing the Spaces Connection to IMAP and SMTP with SSL"](#)
- [Section 33.9, "Securing a Framework Application's Connection to IMAP and SMTP with SSL"](#)
- [Section 33.10, "Securing the Connection to Oracle SES with SSL"](#)
- [Section 33.11, "Securing the Spaces Connection to Microsoft Live Communication Server and Office Communication Server with SSL"](#)
- [Section 33.12, "Securing the Spaces Connection to an External BPEL 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
 - Microsoft Live Communication Server (LCS) - IMP service
 - Oracle WebCenter Portal's Discussion Server - Discussions and Announcements
-
-

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."](#)

33.1 Securing the Browser Connection to Spaces with SSL

Securing the browser connection to Spaces with SSL consists of the following steps:

- [Section 33.1.1, "Creating the Custom Keystore"](#)
- [Section 33.1.2, "Configuring the Custom Identity and Java Trust keystores"](#)
- [Section 33.1.3, "Configuring the SSL Connection"](#)

33.1.1 Creating the Custom Keystore

The first step is to generate a custom keystore for Spaces.

To create a custom keystore:

1. Go to `JDK_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 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 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 WebLogic Server Administration Console.
- b. In the Domain Structure pane, expand Environments and click *Servers*.
- c. In the list of servers, click *WC_Spaces*.
- d. Open the Configuration tab, and the Keystores subtab.

The Keystores Settings pane displays (see [Figure 33–1](#)).

Figure 33–1 Keystores Settings Pane

The screenshot shows the 'Keystores' settings for the 'WLS_Spaces' server. The 'Configuration' tab is active, and the 'Keystores' subtab is selected. The page contains several sections for configuring keystores:

- Keystores:** A dropdown menu is set to 'Custom Identity and Java Standard Trust'.
- Identity Section:**
 - Custom Identity Keystore:** Field contains 'omidks/webcenter_wls.jks'.
 - Custom Identity Keystore Type:** Field contains 'JKS'.
 - Custom Identity Keystore Passphrase:** Field is masked with dots.
 - Confirm Custom Identity Keystore Passphrase:** Field is masked with dots.
- Trust Section:**
 - Java Standard Trust Keystore:** Field contains '/scratch/wcwl/install/0408/wishome/jrockit_160_05_R27.6.2-20/jre/lib/security/cacerts'.
 - Java Standard Trust Keystore Type:** Field contains 'jks'.
 - Java Standard Trust Keystore Passphrase:** Field is empty.
 - Confirm Java Standard Trust Keystore Passphrase:** Field is empty.

A 'Save' button is located at the bottom of the pane.

- e. Note down the location of the server in the **Java Standard Trust Keystore** field (shown in [Figure 33–1](#)).

Note that the *cacerts* file may be "read only", in which case you must 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 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`)

When prompted whether to trust the self-signed certificate, answer yes.

33.1.2 Configuring the Custom Identity and Java Trust Keystores

The next step is to configure the Custom Identity and Java Trust keystores on the Spaces server.

To configure the identity and trust keystores:

1. Log in to the WebLogic Server Administration Console.

For information on logging into the WebLogic Server Administration Console, see [Section 1.13.2, "Oracle WebLogic Server Administration Console."](#)
2. In the Domain Structure pane, expand **Environment** and click **Servers**.

The Summary of Servers pane displays (see [Figure 33–2](#)).

Figure 33–2 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"/>	WC_CustomPortal		LocalMachine	SHUTDOWN		8887
<input type="checkbox"/>	WC_Portlet		LocalMachine	RUNNING	OK	8889
<input type="checkbox"/>	WC_Spaces		LocalMachine	RUNNING	OK	8888

New Clone Delete Showing 1 to 4 of 4 Previous | Next

3. Click the Spaces server (`WC_Spaces`) to configure the identity and trust keystores.

The Settings pane for the Spaces server displays (see [Figure 33–3](#)).

Figure 33–3 Settings Pane for Spaces Server

Settings for WC_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](#)

Name:	WC_Spaces	An alphanumeric name for this server instance. More Info...
Machine:	LocalMachine	The WebLogic Server host computer (machine) on which this server is meant to run. More Info...
Cluster:	(Stand-Alone)	The cluster, or group of WebLogic Server instances, to which this server belongs. More Info...
Listen Address:	<input type="text"/>	The IP address or DNS name this server uses to listen for incoming connections. More Info...
<input checked="" type="checkbox"/> Listen Port Enabled		Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. More Info...
Listen Port:	<input type="text" value="8888"/>	The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. More Info...
<input type="checkbox"/> SSL Listen Port Enabled		Indicates whether the server can be reached through the default SSL listen port. More Info...
SSL Listen Port:	<input type="text" value="8788"/>	The TCP/IP port at which this server listens for SSL connection requests. More Info...
<input type="checkbox"/> Client Cert Proxy Enabled		Specifies whether the HttpClusterServlet proxies the client certificate in a special header. More Info...
Java Compiler:	<input type="text" value="javac"/>	The Java compiler to use for all applications hosted on this server that need to compile Java code. More Info...

4. Open the **Configuration** tab, and then the **Keystores** subtab.

The Keystores pane displays (see [Figure 33–4](#)).

Figure 33–4 Keystores Pane

Settings for WC_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. Under **Identity**, enter the path and filename of the **Custom Identity Keystore** you created in [Section 33.1.1, "Creating the Custom Keystore."](#)
7. Enter **JKS** as the **Custom Identity Keystore Type**.
8. Enter and confirm the **Custom Identity Keystore** password.
9. Under **Trust**, enter and confirm the **Java Standard Trust Keystore** password (typically set to `changeit`).
10. Click **Save** to save your entries.
11. Open the **SSL** tab.
12. Enter the **Private Key Alias** (for example, `webcenter_wls`).
13. Enter the **Private Key Passphrase** (for example, `welcome1`).
14. Click **Save** to save your entries.

33.1.3 Configuring the SSL Connection

To configure the SSL connection:

1. On the Settings pane for the Spaces server, open the Configuration tab and then the General subtab.

The General Configuration pane displays (see [Figure 33–5](#)).

Figure 33–5 General Configuration Pane

Settings for **WC_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](#)

Name:	WC_Spaces	An alphanumeric name for this server instance. More Info...
Machine:	LocalMachine	The WebLogic Server host computer (machine) on which this server is meant to run. More Info...
Cluster:	(Stand-Alone)	The cluster, or group of WebLogic Server instances, to which this server belongs. More Info...
Listen Address:	<input type="text"/>	The IP address or DNS name this server uses to listen for incoming connections. More Info...
<input type="checkbox"/> Listen Port Enabled		Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. More Info...
Listen Port:	<input type="text" value="8888"/>	The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. More Info...
<input checked="" type="checkbox"/> SSL Listen Port Enabled		Indicates whether the server can be reached through the default SSL listen port. More Info...
SSL Listen Port:	<input type="text" value="8788"/>	The TCP/IP port at which this server listens for SSL connection requests. More Info...
<input type="checkbox"/> Client Cert Proxy Enabled		Specifies whether the HttpClusterServlet proxies the client certificate in a special header. More Info...
Java Compiler:	<input type="text" value="javac"/>	The Java compiler to use for all applications hosted on this server that need to compile Java code. More Info...

[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 33–6](#)).

Figure 33–6 Advanced SSL Configuration Settings

Advanced		
Hostname Verification:	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). More Info...
Custom Hostname Verifier:		The name of the class that implements the <code>weblogic.security.SSL.HostnameVerifier</code> interface. More Info...
Export Key Lifespan:	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. More Info...
<input type="checkbox"/> Use Server Certs		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:	Client Certs Not Requested	The form of SSL that should be used. More Info...
Cert Authenticator:		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. More Info...
<input checked="" type="checkbox"/> SSLRejection Logging Enabled		Indicates whether warning messages are logged in the server log when SSL connections are rejected. More Info...
<input type="checkbox"/> Allow Unencrypted Null Cipher		Test if the <code>AllowUnencryptedNullCipher</code> is enabled. More Info...
Inbound Certificate Validation:	Builtin SSL Validation Only	Indicates the client certificate validation rules for inbound SSL. More Info...
Outbound Certificate Validation:	Builtin SSL Validation Only	Indicates the server certificate validation rules for outbound SSL. More Info...
<input type="button" value="Save"/>		

5. Check that the **Two Way Client Cert Behavior** option is set to **Client Certs Not Requested** and click **Save**.
6. Open the Control tab.
The Control Settings pane displays (see [Figure 33–7](#)).

Figure 33–7 Control Settings Pane

Settings for WC_Spaces

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"/>	wc_spaces	LocalMachine	RUNNING	None

Start Resume Suspend ▾ Shutdown ▾ Restart SSL Showing 1 to 1 of 1 Previous | Next

7. Click **Restart SSL**.

8. Restart the WebLogic Server and open the SSL Spaces URL.

For a development or test environment only (that is, not for a production environment), if the hostname in the certificate does not match the host name, then the server must be started with:

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

9. Accept the certificate for the session and log in.

33.2 Securing the Browser Connection to a Framework Application with SSL

Securing the browser connection to a Framework application uses the same configuration steps as for securing the browser connection to Spaces. The only difference is that the configuration occurs on the managed server that is hosting the Framework application deployment rather than the WC_Spaces server. For more information, see [Section 33.1, "Securing the Browser Connection to Spaces with SSL."](#)

33.3 Securing the Connection from Oracle HTTP Server to Spaces with SSL

Securing the connection between the Oracle HTTP Server (OHS) and Spaces is described in the following sections:

- [Section 33.3.1, "Configuring the Identity and Trust Keystores"](#)
- [Section 33.3.2, "Configuring the SSL Connection"](#)
- [Section 33.3.3, "Installing the Oracle HTTP Server"](#)
- [Section 33.3.4, "Wiring the Spaces Ports to the HTTP Server"](#)
- [Section 33.3.5, "Configuring the SSL Certificates"](#)

33.3.1 Configuring the Identity and Trust Keystores

For instructions on how to configure the Identity and Trust keystores, see [Section 33.1, "Securing the Browser Connection to Spaces with SSL."](#)

33.3.2 Configuring the SSL Connection

To configure the SSL Connection:

1. On the Settings pane for the Spaces server, open the Configuration tab and then the General subtab.

The General Configuration pane displays (see [Figure 33–8](#)).

Figure 33–8 General Configuration Pane

Settings for WC_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](#)

Name:	WC_Spaces	An alphanumeric name for this server instance. More Info...
Machine:	LocalMachine	The WebLogic Server host computer (machine) on which this server is meant to run. More Info...
Cluster:	(Stand-Alone)	The cluster, or group of WebLogic Server instances, to which this server belongs. More Info...
Listen Address:	<input type="text"/>	The IP address or DNS name this server uses to listen for incoming connections. More Info...
<input type="checkbox"/> Listen Port Enabled		Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. More Info...
Listen Port:	<input type="text" value="8888"/>	The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. More Info...
<input checked="" type="checkbox"/> SSL Listen Port Enabled		Indicates whether the server can be reached through the default SSL listen port. More Info...
SSL Listen Port:	<input type="text" value="8788"/>	The TCP/IP port at which this server listens for SSL connection requests. More Info...
<input type="checkbox"/> Client Cert Proxy Enabled		Specifies whether the HttpClusterServlet proxies the client certificate in a special header. More Info...
Java Compiler:	<input type="text" value="javac"/>	The Java compiler to use for all applications hosted on this server that need to compile Java code. More Info...

— [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 33–9](#)).

Figure 33–9 Advanced SSL Configuration Settings

Advanced		
Hostname Verification:	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). More Info...
Custom Hostname Verifier:		The name of the class that implements the <code>weblogic.security.SSL.HostnameVerifier</code> interface. More Info...
Export Key Lifespan:	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. More Info...
<input type="checkbox"/> Use Server Certs		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:	Client Certs Not Requested	The form of SSL that should be used. More Info...
Cert Authenticator:		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. More Info...
<input checked="" type="checkbox"/> SSLRejection Logging Enabled		Indicates whether warning messages are logged in the server log when SSL connections are rejected. More Info...
<input type="checkbox"/> Allow Unencrypted Null Cipher		Test if the <code>AllowUnencryptedNullCipher</code> is enabled. More Info...
Inbound Certificate Validation:	Builtin SSL Validation Only	Indicates the client certificate validation rules for inbound SSL. More Info...
Outbound Certificate Validation:	Builtin SSL Validation Only	Indicates the server certificate validation rules for outbound SSL. More Info...
<input type="button" value="Save"/>		

- Set the **Two Way Client Cert Behavior** option to `Client Certs Not Requested` and click **Save**.
- Open the Control tab on the Settings pane, and select the Start/Stop subtab.
- Click **Restart SSL**.
- Open the SSL Spaces URL.
- Accept the certificate for the session and log in.
- In the WSL Administration Console, click **View Changes and Restarts** on the Change Center pane and restart any affected servers or components.

33.3.3 Installing the Oracle HTTP Server

To install the Oracle HTTP Server:

- Install the WebTier.
 - Do not select WebCache; only select the HTTP Server.
 - Uncheck the checkbox to associate a WebLogic server during install.
- Navigate to the `WT_ORACLE_HOME/instances/<your_instance>/bin` directory and start OHS using the following command:


```
./opmnctl startall
```

3. Check the status of OHS using the following command:

```
./opmnctl status -l
```

33.3.4 Wiring the Spaces Ports to the HTTP Server

To wire the Spaces ports to the HTTP server:

1. Open the file

```
WT_ORACLE_HOME/instances/<your_instance>/config/OHS/ohs1/mod_wl_ohs.conf.
```

2. Add the following entry to `mod_wl_ohs.conf` to make 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 Spaces server ID and port number.

3. Open the file

```
WT_ORACLE_HOME/instances/<your_instance>/config/OHS/ohs1/ssl.conf.
```

4. Add the following entry to `ssl.conf` to make Spaces run on the OHS SSL port:

```
<Location />
    WebLogicHost host_id
    WebLogicPort port
    SetHandler weblogic-handler
    SecureProxy ON
    WLLogFile /tmp/ohs_ssl.log
    Debug ALL
    WlSSLWallet SSL_wallet
</Location>

<Location /webcenter>
    SetHandler weblogic-handler
    WebLogicHost host_id
    WebLogicPort port
    SecureProxy ON
    WLLogFile /tmp/ohs_ssl.log
    Debug ALL
    WlSSLWallet SSL_wallet
</Location>

<Location /webcenterhelp>
    SetHandler weblogic-handler
    WebLogicHost host_id
    WebLogicPort port
    SecureProxy ON
    WLLogFile /tmp/ohs_ssl.log
```

```

        Debug ALL
        WLSSEWallet SSL_wallet
    </Location>

    <Location /rsscrawl>
        SetHandler weblogic-handler
        WebLogicHost host_id
        WebLogicPort port
        SecureProxy ON
        WLSSEWallet /tmp/ohs_ssl.log
        Debug ALL
        WLSSEWallet SSL_wallet
    </Location>

    <Location /sesUserAuth>
        SetHandler weblogic-handler
        WebLogicHost host_id
        WebLogicPort port
        SecureProxy ON
        WLSSEWallet /tmp/ohs_ssl.log
        Debug ALL
        WLSSEWallet SSL_wallet
    </Location>

    <Location /rss>
        SetHandler weblogic-handler
        WebLogicHost host_id
        WebLogicPort port
        SecureProxy ON
        WLSSEWallet /tmp/ohs_ssl.log
        Debug ALL
        WLSSEWallet SSL_wallet
    </Location>

```

Replacing *host_id* and *port* with the WebCenter Portal SSL server ID and port number (typically 8788), and *SSL_wallet* with the path to the WebLogic SSL wallet (for example, `WT_ORACLE_HOME/instances/<your_instance>/config/OHS/ohs1/keys/tores/default`).

Note: SSL should be configured at the server level rather than within the Location/directory sections. So, for example, instead of having:

```

<Location /mylocation>
    WLSSEWallet <walletfile>
    SecureProxy ON
</Location>

```

use:

```

SecureProxy ON
WLSSEWallet <walletfile>

```

at the server level (i.e., outside the Location/directory sections).

5. Go to `WT_ORACLE_HOME/instances/<your_instance>/bin` and start and check the status of OHS using the following commands:

```

./opmnctl stopall

```

```
./opmnctl startall
./opmnctl status -l
```

33.3.5 Configuring the SSL Certificates

To configure the SSL certificates:

1. For OHS to trust WebCenter Portal's certificate, the `WC_Spaces` certificate must be imported into the OHS trust store. Export the certificate from the `WC_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 Portal 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 `WC_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 `WC_Spaces` server.

You should now be able to access the SSL OHS, as well as the non-SSL OHS.

33.4 Securing the Browser Connection to the Discussions Service with SSL

Securing the browser connection to the Discussions service with SSL is described in the following sections:

- [Section 33.4.1, "Creating the Custom Keystore"](#)
- [Section 33.4.2, "Configuring the Identity and Trust Key Stores"](#)
- [Section 33.4.3, "Configuring the SSL Connection"](#)

33.4.1 Creating the Custom Keystore

The first step is to generate a custom keystore as shown below:

1. Go to `JDK_HOME/bin/` and open a command prompt.
2. Using `keytool`, generate a key pair:

```
keytool -genkeypair -keyalg RSA -dname "dname" -alias owc_discussions
-keypass key_password -keystore owc_discussions.jks -storepass
keystore_password -validity days_valid
```

Where:

- *dname* is the DN (distinguished name) to use (for example, `cn=customidentity,dc=owc_discussions,dc=example,dc=com`)
- *key_password* is the password for the new public key, (for example, `welcome1`)
- *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:

```
keytool -exportcert -v -alias owc_discussions -keystore owc_discussions.jks  
-storepass keystore_password -rfc -file owc_discussions.cer
```

Where:

- *keystore_password* is the keystore password, (for example, `welcome1`)

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 WebLogic Server Administration Console.
- b. In the Domain Structure pane, expand Environments and click `Servers`.
- c. In the list of servers, click `WC_Collaboration`.
- d. Open the Configuration tab, and the Keystores subtab.

The Keystores Settings pane displays (see [Figure 33-10](#)).

Figure 33–10 Keystores Subtab for WC_Collaboration

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: /path/owc_discussions.jks The path and file name of the identity keystore. [More Info...](#)

Custom Identity Keystore Type: JKS The type of the keystore. Generally, this is JKS. [More Info...](#)

Custom Identity Keystore Passphrase: [Masked] 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: [Masked]

— Trust —

Java Standard Trust Keystore: /scratch/PS1fmwhome/jdk160_14_R27.6.5-32/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: [Masked] 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: [Masked]

Save

- e. Note down the location of the server in the **Java Standard Trust Keystore** field (shown in [Figure 33–1](#)).

Note that the `cacerts` file may be "read only", in which case you must change its permissions so that it's writable.

5. Import the self-signed certificate generated above in this trust store:

```
keytool -importcert -trustcacerts -alias owc_discussions
-file owc_discussions.cer -keystore cacerts -storepass changeit
```

When prompted to trust the self-signed certificate, say yes.

33.4.2 Configuring the Identity and Trust Key Stores

To configure the identity and trust key stores:

1. Log in to the WebLogic Server Administration Console.

For information on logging into the WebLogic Server Administration Console, see [Section 1.13.2, "Oracle WebLogic Server Administration Console."](#)

2. In the Domain Structure pane, expand **Environment** and click **Servers**.

The Summary of Servers pane displays (see [Figure 33–11](#)).

Figure 33–11 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"/>	WC_Portlet			RUNNING	✔ OK	8889
<input type="checkbox"/>	WC_Collaboration			RUNNING	✔ OK	8890
<input type="checkbox"/>	WC_Spaces			RUNNING	✔ OK	8888

New Clone Delete Showing 1 to 4 of 4 Previous | Next

3. Click the Collaboration server (WC_Collaboration) to configure the identity and trust keystores.

The Settings pane for the services server displays (see [Figure 33–12](#)).

Figure 33–12 Settings Pane for Services Server

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	
<input type="button" value="Save"/>		
Use this page to configure general features of this server such as default network communications.		
View JNDI Tree		
Name:	WC_Collaboration	An alphanumeric name for this server instance. More Info...
Machine:	(None)	The WebLogic Server host computer (machine) on which this server is meant to run. More Info...
Cluster:	(Stand-Alone)	The cluster, or group of WebLogic Server instances, to which this server belongs. More Info...
Listen Address:	<input type="text"/>	The IP address or DNS name this server uses to listen for incoming connections. More Info...
<input checked="" type="checkbox"/> Listen Port Enabled		Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. More Info...
Listen Port:	<input type="text" value="8890"/>	The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. More Info...
<input type="checkbox"/> SSL Listen Port Enabled		Indicates whether the server can be reached through the default SSL listen port. More Info...
SSL Listen Port:	<input type="text" value="8790"/>	The TCP/IP port at which this server listens for SSL connection requests. More Info...
<input type="checkbox"/> Client Cert Proxy Enabled		Specifies whether the HttpClusterServlet proxies the client certificate in a special header. More Info...
Java Compiler:	<input type="text" value="javac"/>	The Java compiler to use for all applications hosted on this server that need to compile Java code. More Info...
Advanced		
<input type="button" value="Save"/>		

4. Open the **Configuration** tab, and then the **Keystores** subtab.
The Keystores pane displays (see [Figure 33–13](#)).

Figure 33–13 Keystores Pane

The screenshot shows the 'Settings for WC Collaboration' interface. The 'Configuration' tab is selected, and the 'Keystores' subtab is active. A 'Save' button is at the top left. Below it is a descriptive paragraph: '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.'

The 'Keystores:' section has a dropdown menu set to 'Custom Identity and Java Standard Trust'. To its right is a question: 'Which configuration rules should be used for finding the server's identity and trust keystores?' with a 'More Info...' link.

Under the 'Identity' section, there are four rows of configuration fields:

- Custom Identity Keystore:** An empty text box. Description: 'The path and file name of the identity keystore. More Info...'
- Custom Identity Keystore Type:** An empty text box. Description: 'The type of the keystore. Generally, this is JKS. More Info...'
- Custom Identity Keystore Passphrase:** An empty text box. Description: '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:** An empty text box.

Under the 'Trust' section, there are four rows of configuration fields:

- Java Standard Trust Keystore:** A text box containing the path: `/u01/app/oracle/product/IR13/fmwhome/jrockit_160_05_R27.6.2-20/jre/lib/security/cacerts`. Description: 'The path and file name of the trust keystore. More Info...'
- Java Standard Trust Keystore Type:** A text box containing 'jks'. Description: 'The type of the keystore. Generally, this is JKS. More Info...'
- Java Standard Trust Keystore Passphrase:** An empty text box. Description: '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:** An empty text box.

A 'Save' button is located at the bottom left of the configuration area.

5. For **Keystores**, select **Custom Identity and Java Standard Trust**.
6. Under **Identity**, specify the keystore as `owc_discussions.jks`.
7. Set the keystore type to **JKS**.
8. Enter and confirm the keystore passphrase, (for example, `welcome1`)
9. Under **Trust**, set the **Java Standard Trust Keystore Passphrase** to `changeit` (this is fixed value) and click **Save**.
10. From the WLS Administration console, go to **Servers -> WC_Collaboration** and open the **Configuration** tab, and then the **General** subtab.
11. Check **SSL Port enabled**, specify a port that you want, and save your settings.
12. From the WLS Administration console, go to **Servers -> WC_Collaboration** and open the **Configuration** tab, and then the **SSL** subtab.
13. Specify the private key alias as `owc_discussions`, and set the password to `welcome1`.
14. Open the **Control** tab.

The **Control** Settings pane displays (see [Figure 33–14](#)).

Figure 33–14 Control Settings Pane

Settings for WC_Collaboration

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"/>	WC Collaboration		RUNNING	None

Start Resume Suspend ▾ Shutdown ▾ Restart SSL Showing 1 to 1 of 1 Previous | Next

15. Click **Restart SSL**.

33.4.3 Configuring the SSL Connection

To 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 33–15](#)).

Figure 33–15 General Configuration Pane

Settings for WC_Collaboration

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](#)

Name:	WC_Collaboration	An alphanumeric name for this server instance. More Info...
Machine:	LocalMachine	The WebLogic Server host computer (machine) on which this server is meant to run. More Info...
Cluster:	(Stand-Alone)	The cluster, or group of WebLogic Server instances, to which this server belongs. More Info...
Listen Address:	<input type="text"/>	The IP address or DNS name this server uses to listen for incoming connections. More Info...
<input type="checkbox"/> Listen Port Enabled		Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. More Info...
Listen Port:	<input type="text" value="8888"/>	The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. More Info...
<input checked="" type="checkbox"/> SSL Listen Port Enabled		Indicates whether the server can be reached through the default SSL listen port. More Info...
SSL Listen Port:	<input type="text" value="8788"/>	The TCP/IP port at which this server listens for SSL connection requests. More Info...
<input type="checkbox"/> Client Cert Proxy Enabled		Specifies whether the HttpClusterServlet proxies the client certificate in a special header. More Info...
Java Compiler:	<input type="text" value="javac"/>	The Java compiler to use for all applications hosted on this server that need to compile Java code. More Info...

— **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 33–16](#)).

Figure 33–16 Advanced SSL Configuration Settings

Advanced		
Hostname Verification:	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). More Info...
Custom Hostname Verifier:		The name of the class that implements the <code>weblogic.security.SSL.HostnameVerifier</code> interface. More Info...
Export Key Lifespan:	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. More Info...
<input type="checkbox"/> Use Server Certs		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:	Client Certs Not Requested	The form of SSL that should be used. More Info...
Cert Authenticator:		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. More Info...
<input checked="" type="checkbox"/> SSLRejection Logging Enabled		Indicates whether warning messages are logged in the server log when SSL connections are rejected. More Info...
<input type="checkbox"/> Allow Unencrypted Null Cipher		Test if the <code>AllowUnEncryptedNullCipher</code> is enabled. More Info...
Inbound Certificate Validation:	Builtin SSL Validation Only	Indicates the client certificate validation rules for inbound SSL. More Info...
Outbound Certificate Validation:	Builtin SSL Validation Only	Indicates the server certificate validation rules for outbound SSL. More Info...
Save		

5. Set the **Two Way Client Cert Behavior** option to `Client Certs Not Requested` and click **Save**.
6. Restart the `WC_Collaboration` server and open the SSL Discussions URL at `https://host:port/owc_discussions`.
7. Accept the certificate for the session and log in.

33.5 Securing the Spaces Connection to Portlet Producers with SSL

Securing the connection to WSRP and PDK-Java portlet producers with SSL is described in the following sections:

- [Section 33.5.1, "Configuring the Identity and Trust Key Stores"](#)
- [Section 33.5.2, "Configuring the SSL Connection"](#)
- [Section 33.5.3, "Registering the SSL-enabled WSRP Producer and Running the Portlets"](#)
- [Section 33.5.4, "Registering the SSL-enabled PDK-Java Producer and Running the Portlets"](#)

33.5.1 Configuring the Identity and Trust Key Stores

To configure the identity and trust key stores:

1. Log in to the WebLogic Server Administration Console.
For information on logging into the WebLogic Server Administration Console, see [Section 1.13.2, "Oracle WebLogic Server Administration Console."](#)
2. In the Domain Structure pane, expand **Environment** and click **Servers**.
The Summary of Servers pane displays (see [Figure 33–17](#)).

Figure 33–17 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"/>	WC_CustomPortal		LocalMachine	SHUTDOWN		8887
<input type="checkbox"/>	WC_Portlet		LocalMachine	RUNNING	✔ OK	8889
<input type="checkbox"/>	WC_Spaces		LocalMachine	RUNNING	✔ OK	8888

New Clone Delete Showing 1 to 4 of 4 Previous | Next

3. Click the Portlet server (for example, `WC_Portlet`) to configure the identity and trust keystores.

The Settings pane for the Portlet server displays (see [Figure 33–18](#)).

Figure 33–18 Settings Pane for Portlet Server

Settings for WC_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](#)

Name:	WC_Spaces	An alphanumeric name for this server instance. More Info...
Machine:	LocalMachine	The WebLogic Server host computer (machine) on which this server is meant to run. More Info...
Cluster:	(Stand-Alone)	The cluster, or group of WebLogic Server instances, to which this server belongs. More Info...
Listen Address:	<input type="text"/>	The IP address or DNS name this server uses to listen for incoming connections. More Info...
<input checked="" type="checkbox"/> Listen Port Enabled		Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. More Info...
Listen Port:	<input type="text" value="8888"/>	The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. More Info...
<input type="checkbox"/> SSL Listen Port Enabled		Indicates whether the server can be reached through the default SSL listen port. More Info...
SSL Listen Port:	<input type="text" value="8788"/>	The TCP/IP port at which this server listens for SSL connection requests. More Info...
<input type="checkbox"/> Client Cert Proxy Enabled		Specifies whether the HttpClusterServlet proxies the client certificate in a special header. More Info...
Java Compiler:	<input type="text" value="javac"/>	The Java compiler to use for all applications hosted on this server that need to compile Java code. More Info...

4. Open the **Configuration** tab, and then the **Keystores** subtab.

The Keystores pane displays (see [Figure 33–19](#)).

Figure 33–19 Keystores Pane

Settings for WC_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/frmwhome/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 33–20](#)).

Figure 33–20 Control Settings Pane

Settings for WC_Spaces

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"/>	wc_spaces	LocalMachine	RUNNING	None

Start Resume Suspend ▾ Shutdown ▾ Restart SSL Showing 1 to 1 of 1 Previous | Next

7. Click **Restart SSL**.

33.5.2 Configuring the SSL Connection

To configure the SSL connection:

1. In the Domain Structure pane, expand **Environment** and select **Servers**.
2. Click the Portlet server (for example, `WC_Utilities`) 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.

33.5.3 Registering the SSL-enabled WSRP Producer and Running the Portlets

To register the SSL-enabled WSRP producer and run the portlets:

1. Configure the Spaces managed server to use the Custom Identity and Java Standard Trust store. This also uses the certificates in `JDK_HOME/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 WebLogic Server `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 `JDK_HOME/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 `WC_Spaces`.
 5. Start WLST as described in [Section 1.13.3.1, "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 `WC_Spaces` server (for example, `weblogic`)
 - `password` is the password with which to access the `WC_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?WSDL')
```

8. Navigate to the HTTP or HTTPS WebCenter Portal 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.

33.5.4 Registering the SSL-enabled PDK-Java Producer and Running the Portlets

To register the SSL-enabled PDK-Java Producer and run the portlets:

1. Configure the Spaces managed server to use the Demo Identity and Trust store. This also uses the certificates in `JDK_HOME/jre/lib/security/cacerts`.
2. Log in to the WebLogic Server Administration Console.

For information on logging into the WebLogic Server Administration Console, see [Section 1.13.2, "Oracle WebLogic Server Administration Console."](#)

3. On the Domain Structure pane, expand **Environment** and click **Servers**.
The Summary of Servers pane displays (see [Figure 33–21](#)).

Figure 33–21 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"/>	WC_CustomPortal		LocalMachine	SHUTDOWN		8887
<input type="checkbox"/>	WC_Portlet		LocalMachine	RUNNING	✔ OK	8889
<input type="checkbox"/>	WC_Spaces		LocalMachine	RUNNING	✔ OK	8888

New Clone Delete Showing 1 to 4 of 4 Previous | Next

4. Click `WC_Spaces` in the servers list.
The Settings pane displays (see [Figure 33–22](#)).

Figure 33–22 Settings Pane (WC_Spaces Server)

Settings for WC_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/frmwhome/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. Open the Configuration tab and select the Keystores tab.
6. Make sure that the value for **Demo Identity and Demo Trust** is either `jkcs` 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 WebLogic Server `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 `JDK_HOME/jre/lib/security` using the following keytool command:


```
keytool -importcert HOME/portlet_cert.pem -keystore ./cacerts -storepass changeit
```
10. Restart WC_Spaces.
11. Start WLST as described in [Section 1.13.3.1, "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 WC_Spaces server (for example, weblogic)
- *password* is the password with which to access the WC_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 enables 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 Portal 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.

33.6 Securing the 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 Portal, the identity store should be configured for authentication with the appropriate authenticator. See [Chapter 29, "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:

- [Section 33.6.1, "Exporting the OID Certificate Authority \(CA\)"](#)
- [Section 33.6.2, "Setting Up the WebLogic Server"](#)

33.6.1 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 must 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
```

33.6.2 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
```

33.7 Securing the Spaces Connection to Content Server with SSL

If Content Server and the Spaces 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 secure identity propagation you must also configure SSL on Content Server.

Securing Content Server with SSL involves the following tasks:

- [Section 33.7.1, "Configuring a Keystore and Key on the Client Side"](#)
- [Section 33.7.2, "Configuring a Keystore and Key on the Server Side"](#)
- [Section 33.7.3, "Verifying Signatures of Trusted Clients"](#)
- [Section 33.7.4, "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. 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.

33.7.1 Configuring a Keystore and Key on the Client Side

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

1. Go to the location, for example `jdk/bin`, where the `keytool` is located, 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
```

33.7.2 Configuring a Keystore and Key on the Server Side

To configure a keystore on the Content Server side:

1. Go to the location, for example `jdk/bin`, where the keytool is located, 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
```

33.7.3 Verifying Signatures of Trusted Clients

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

1. Go to the location, for example `jdk/bin`, where the keytool is located, 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 33-1](#) shows a sample output that is generated after this procedure is completed successfully.

Example 33-1 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.
```

33.7.4 Securing Identity Propagation

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

1. Log on to 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 33–2](#) shows how the `.hda` file should look after you include the truststore and keystore information.

Example 33–2 Sample `sslconfig.hda` File

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

33.8 Securing the Spaces Connection to IMAP and SMTP with SSL

Before reconfiguring the mail server connection, you must first import the certificate into the trust store. Follow the steps below to put the certificate in the trust store and configure Spaces to use the trust store.

To secure the 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 WebLogic Server `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 17.4, "Registering Mail Servers."](#)
8. Restart Spaces.

9. Log into Spaces and provide your mail credentials.

33.9 Securing a Framework Application's Connection to IMAP and SMTP with SSL

To secure the connection to IMAP and SMTP with SSL for a Framework application:

1. Follow the steps in [Section 33.8, "Securing the Spaces Connection to IMAP and SMTP with SSL"](#) up to and including step 7.
2. Add the following property to the truststore:

```
-Djavax.net.ssl.trustStore=C:\jive\mailtool\jssecacerts
-Djavax.net.ssl.trustStorePassword=changeit
```

For example:

```
set JAVA_PROPERTIES=-Dplatform.home=%WL_HOME% -Dwls.home=%WLS_HOME%
-Dweblogic.home=%WLS_HOME%
-Djavax.net.ssl.trustStore=C:\jive\mailtool\jssecacerts
-Djavax.net.ssl.trustStorePassword=changeit
```

3. Restart the Framework application.
4. Log into the application and provide your mail credentials.

33.10 Securing the Connection to Oracle SES with SSL

Before registering the SES connection, you must 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 WebLogic Server `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 22.4.1, "Registering Oracle Secure Enterprise Search Servers."](#)
8. Restart Spaces or Framework application.

33.11 Securing the Spaces Connection to Microsoft Live Communication Server and Office Communication Server with SSL

To secure the Spaces connection to Microsoft Live Communication Server (LCS) or Office Communication Server 2007 (OCS) with SSL, follow the steps below to import the certificate into the trust store, and point Spaces to use the trust store. Note that securing the Spaces connection to Microsoft Live Communication Server or Office Communication Server with SSL is optional since they can be configured with confidentiality using WS-Security.

Before registering the LCS or OCS connection, you must first import the certificate into the trust store. Follow the steps below to put the certificate in the trust store:

1. Open your browser and go to the communication server (for example, <https://example.com/RTC>)
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 WebLogic Server `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 communication server in the installation, and also update the communication server referenced `cacerts` file with this certificate:

```
keytool -import -alias lcs_cer -file cert_file.cer -keystore cacerts -storepass changeit
```

7. Register the communication server connection as described in [Section 16.3, "Registering Instant Messaging and Presence Servers."](#)
8. Restart the Spaces server.

33.12 Securing the Spaces Connection to an External BPEL Server with SSL

This section describes how to secure the Spaces connection to a BPEL server when the BPEL server resides in an external SOA domain.

Note: When SOA is installed in an external domain, the Identity Asserter and Authenticator should be configured exactly as for WebCenter Portal. For more information on configuring the Identity Asserter and Authenticator for an external LDAP identity store, see [Section 29.1, "Reassociating the Identity Store with an External LDAP Server."](#)

To secure the Spaces connection to an external BPEL server with SSL:

1. Copy the public certificate (`webcenter_wls.cer`) from WebCenter Portal into the SOA domain.
2. Go to `JDK_HOME/bin/` and open a command prompt.
3. Generate a custom keystore on the SOA domain naming the keystore `soa_server1.jks`, and the alias `soa_server1` using the following `keytool` command:

```
keytool -genkeypair -keyalg RSA -dname dname -alias soa_server1 -keypass key_pass -keystore soa_server1.jks -storepass keystore_password -validity days_valid
```

Where:

- *dname* is the DN (distinguished name) to use (for example, `cn=customidentity,dc=example,dc=com`)
 - *key_pass* is the password for the new public key, (for example, `welcome1`)
 - *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`).
4. Export the certificate from `soa_wls.jks` using the following command:

```
keytool -exportcert -v -alias soa_server1 -keystore soa_server1.jks -storepass keystore_password -rfc -file soa_server1.cer
```

Where:

- *keystore_password* is the keystore password, (for example, `welcome1`)
5. Log in to the WebLogic Server Administration Console on the SOA domain.
For information on logging into the WebLogic Server Administration Console, see [Section 1.13.2, "Oracle WebLogic Server Administration Console."](#)
 6. In the Navigation pane, expand **Environment** and click **Servers**.
The Summary of Servers pane displays (see [Figure 33–23](#)).

Figure 33–23 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 2 of 2 Previous | Next

<input type="checkbox"/>	Name ↕	Cluster	Machine	State	Health	Listen Port
<input type="checkbox"/>	AdminServer(admin)			RUNNING	✔ OK	7001
<input type="checkbox"/>	soa_server1		LocalMachine	RUNNING	✔ OK	8001

New Clone Delete Showing 1 to 2 of 2 Previous | Next

7. From the Configuration tab, click `soa_server1` in the list of servers. The Settings page for `soa_server1` displays (see [Figure 33–24](#)).

Figure 33–24 Settings Page for soa_server1

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

Save

Use this page to configure general features of this server such as default network communications.

[View JNDI Tree](#)

Name:	soa_server1	An alphanumeric name for this server instance. More Info...
Machine:	LocalMachine	The WebLogic Server host computer (machine) on which this server is meant to run. More Info...
Cluster:	(Standalone)	The cluster, or group of WebLogic Server instances, to which this server belongs. More Info...
Listen Address:	<input type="text"/>	The IP address or DNS name this server uses to listen for incoming connections. More Info...
<input type="checkbox"/> Listen Port Enabled		Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. More Info...
Listen Port:	<input type="text" value="8001"/>	The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. More Info...
<input checked="" type="checkbox"/> SSL Listen Port Enabled		Indicates whether the server can be reached through the default SSL listen port. More Info...
SSL Listen Port:	<input type="text" value="8002"/>	The TCP/IP port at which this server listens for SSL connection requests. More Info...
<input type="checkbox"/> Client Cert Proxy Enabled		Specifies whether the HttpClusterServlet proxies the client certificate in a special header. More Info...
Java Compiler:	<input type="text" value="javac"/>	The Java compiler to use for all applications hosted on this server that need to compile Java code. More Info...

[Advanced](#)

Save

- Open the Keystores tab.

The Keystore settings for soa_server1 displays (see [Figure 33–25](#)).

Figure 33–25 Keystore Settings for soa_server1

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

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: /path/soa_server1.jks The path and file name of the identity keystore. [More Info...](#)

Custom Identity Keystore Type: JKS 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: /path/jdk160_14_R27.6.5-32/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

9. For **Keystores**, select Custom Identity and Java Standard Trust.
10. Specify the path and filename of keystore (`soa_server1.jks`) created above.
11. Go to the directory containing the java standard trust (`cacerts` file) specified in the **Java Standard Trust Keystores** field and import the SOA and WebCenter Portal public certificates into this file so they may be trusted by the server:

```
keytool -importcert -trustcacerts -alias webcenter_wls -file webcenter_wls.cer
-keystore cacerts -storepass keystore_password
```

```
keytool -importcert -trustcacerts -alias soa_server1 -file soa_server1.cer
-keystore cacerts -storepass keystore_password
```

Where:

- `keystore_password` is the keystore password, (for example, `welcome1`)
- Say yes when prompted to trust the certificate.

12. From the WLS Administration Console on the SOA domain, open the SSL tab.

The SSL settings for `soa_server1` display (see [Figure 33–26](#)).

Figure 33–26 SSL Settings for soa_server1

The screenshot shows the 'Settings for soa_server1' configuration page with the 'SSL' tab selected. The page includes a 'Save' button at the top left and a descriptive paragraph: 'This page lets you view and define various Secure Sockets Layer (SSL) settings for this server instance. These settings help you to manage the security of message transmissions.'

Identity and Trust Locations: A dropdown menu is set to 'Keystores'. Description: 'Indicates where SSL should find the server's identity (certificate and private key) as well as the server's trust (trusted CAs). [More Info...](#)'

Private Key Location: 'from Custom Identity Keystore'. Description: 'The keystore attribute that defines the location of the private key file. [More Info...](#)'

Private Key Alias: 'soa_server1'. Description: 'The keystore attribute that defines the string alias used to store and retrieve the server's private key. [More Info...](#)'

Private Key Passphrase: A password field with 12 dots. Description: 'The keystore attribute that defines the passphrase used to retrieve the server's private key. [More Info...](#)'

Confirm Private Key Passphrase: A password field with 12 dots.

Certificate Location: 'from Custom Identity Keystore'. Description: 'The keystore attribute that defines the location of the trusted certificate. [More Info...](#)'

Trusted Certificate Authorities: 'from Java Standard Trust Keystore'. Description: 'The keystore attribute that defines the location of the certificate authorities. [More Info...](#)'

At the bottom, there is an 'Advanced' section with a right-pointing arrow and another 'Save' button.

13. Specify soa_server1 as the **Private Key Alias**.
14. Enter and confirm the password for the private key (for example, welcome1) and click **Save**.
15. Open the General tab.

The General settings for soa_server1 display (see [Figure 33–27](#)).

Figure 33–27 General Settings for soa_server1

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

Save

Use this page to configure general features of this server such as default network communications.

[View JNDI Tree](#)

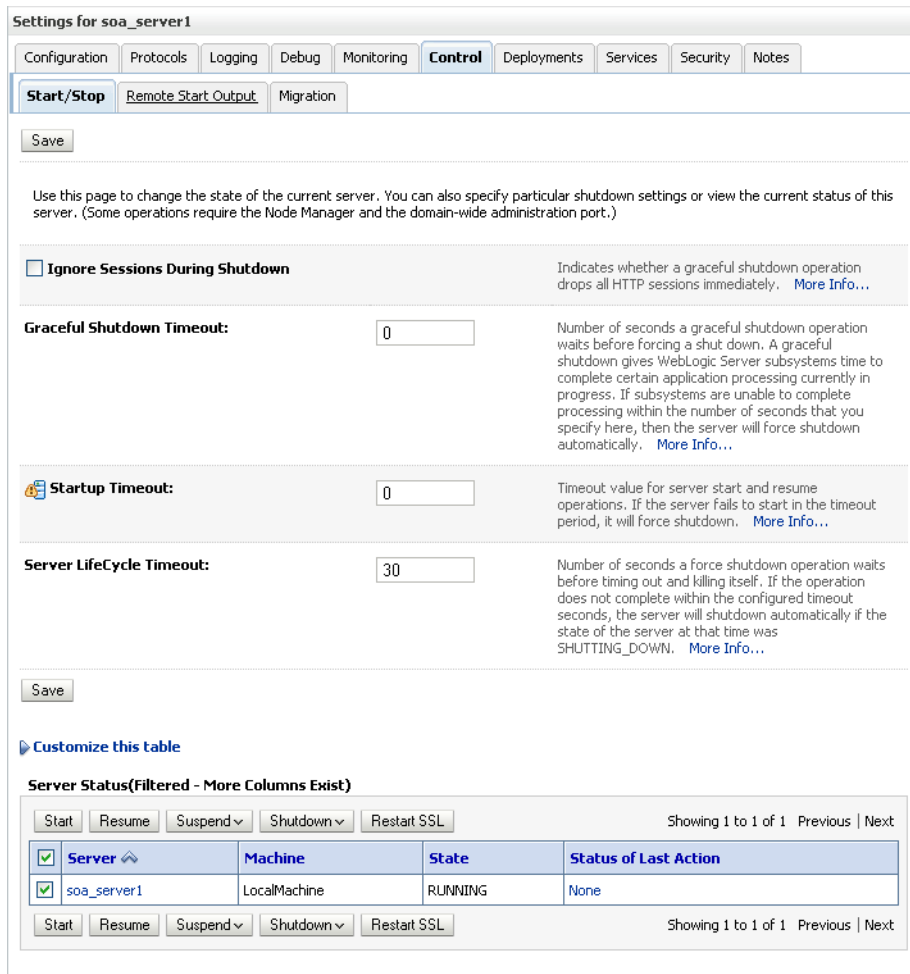
Name:	soa_server1	An alphanumeric name for this server instance. More Info...
Machine:	LocalMachine	The WebLogic Server host computer (machine) on which this server is meant to run. More Info...
Cluster:	(Standalone)	The cluster, or group of WebLogic Server instances, to which this server belongs. More Info...
Listen Address:	<input type="text"/>	The IP address or DNS name this server uses to listen for incoming connections. More Info...
<input type="checkbox"/> Listen Port Enabled		Specifies whether this server can be reached through the default plain-text (non-SSL) listen port. More Info...
Listen Port:	<input type="text" value="8001"/>	The default TCP port that this server uses to listen for regular (non-SSL) incoming connections. More Info...
<input checked="" type="checkbox"/> SSL Listen Port Enabled		Indicates whether the server can be reached through the default SSL listen port. More Info...
SSL Listen Port:	<input type="text" value="8002"/>	The TCP/IP port at which this server listens for SSL connection requests. More Info...
<input type="checkbox"/> Client Cert Proxy Enabled		Specifies whether the HttpClusterServlet proxies the client certificate in a special header. More Info...
Java Compiler:	<input type="text" value="javac"/>	The Java compiler to use for all applications hosted on this server that need to compile Java code. More Info...

— **Advanced**

Save

16. Make sure that **Listen Port Enabled** is not selected.
17. Select **SSL Listen Port Enabled**, specify the **SSL Listen Port**, and click **Save**.
18. Open the **Control** tab, and then open the **Start/Stop** sub-tab.
The Start/Stop settings for soa_server1 display (see [Figure 33–28](#)).

Figure 33–28 Start/Stop Settings for soa_server1



19. Select soa_server1 from the list of servers, and click **Restart SSL**.
20. Restart the soa_server1 Managed Server on the SOA domain.
21. From the WebCenter Portal domain, import the soa_server1.cer certificate as a trusted certificate to the server trust store (cacerts) using the following keytool commands:


```
keytool -importcert -trustcacerts -alias soa_server1 -file soa_server1.cer -keystore cacerts -storepass changeit
```

Say yes when prompted to trust the certificate.
22. Add the Worklist connection on the WebCenter Portal domain as described in [Section 23.4.2, "Registering Worklist Connections"](#) specifying the host:ssl_port settings for soa_server1 when defining the BPEL URL.
23. Restart the WC_Spaces Managed Server.

Configuring WS-Security

This chapter describes how to set up WS-Security for WebCenter Portal applications (including Spaces and Framework applications) and related services and components based on your topology. This section covers the following configurations:

- A simple topology, with the WebCenter Portal application and all components sharing the same domain
- A typical topology, with the WebCenter Portal application and components divided across two domains
- A complex topology, with the WebCenter Portal application and components divided across multiple domains

Within these three topologies, configuration is described for the WebCenter Portal application (Spaces, for example), Oracle WebCenter Portal's Discussion Server, the Worklist service, and WSRP producers. These configurations and the steps for securing applications consuming Spaces APIs are covered in the following sections:

- [Section 34.1, "Configuring WS-Security for a Simple Topology"](#)
- [Section 34.2, "Configuring WS-Security for a Typical Topology"](#)
- [Section 34.3, "Configuring WS-Security for a Complex Topology"](#)
- [Section 34.4, "Securing Spaces for Applications Consuming Spaces Client APIs with WS-Security"](#)

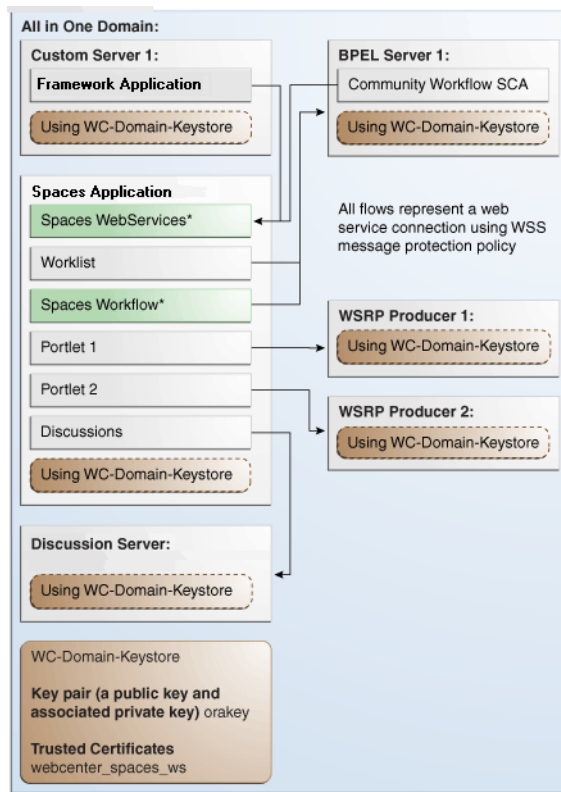
Audience

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."](#)

34.1 Configuring WS-Security for a Simple Topology

This section describes how to configure WS-Security for a topology where the WebCenter Portal applications, the BPEL server, and WSRP producers share the same domain ([Figure 34-1](#)).

Figure 34–1 WS-Security for a Simple Configuration



*applicable to Spaces application only

The steps to configure WS-Security for a simple single-domain WebCenter Portal topology are described in the following sections:

- [Section 34.1.1, "Roadmap to Configuring WS-Security for a Simple Topology"](#)
- [Section 34.1.2, "Setting Up the WebCenter Portal Domain Keystore"](#)
- [Section 34.1.3, "Configuring the Discussions Server for a Simple Topology"](#)
- [Section 34.1.4, "Command Summary for a Simple Topology"](#)

34.1.1 Roadmap to Configuring WS-Security for a Simple Topology

The flow chart (Figure 34–1) and table (Table 34–1) in this section provide an overview of the prerequisites and tasks required to configure WS-Security for a simple single-domain WebCenter Portal topology.

Figure 34–2 Configuring WS-Security for a Simple Topology

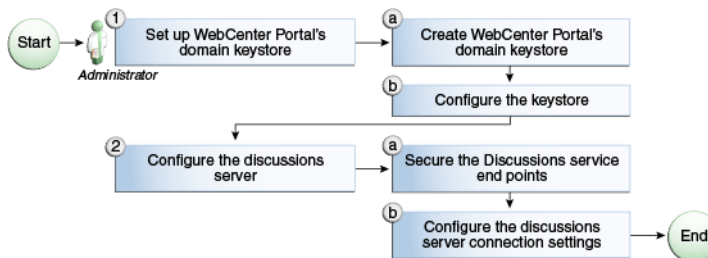


Table 34–1 shows the tasks and sub-tasks to configure WS-Security for a simple WebCenter Portal topology.

Table 34–1 Configuring WS-Security for a Simple Topology

Actor	Task	Sub-task	Notes
Administrator	1. Set up the WebCenter Portal domain keystore	1.a Create the WebCenter Portal domain keystore	
		1.b Configure the keystore	
	2. Configure the discussions server	2.a Secure the Discussions service end points	
		2.b Configure the discussions server connection settings	

34.1.2 Setting Up the WebCenter Portal Domain Keystore

The security credentials of the WebCenter Portal application, discussions server, BPEL server, and WSRP producers 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.

This section contains the following subsections:

- [Section 34.1.2.1, "Creating the WebCenter Portal Domain Keystore"](#)
- [Section 34.1.2.2, "Configuring the Keystore with WLST"](#)
- [Section 34.1.2.3, "Configuring the Keystore Using Fusion Middleware Control"](#)

34.1.2.1 Creating the WebCenter Portal Domain Keystore

This section describes how to create a keystore 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 the WebCenter Portal domain keystore:

1. Go to `JDK_HOME/jdk/bin` and open a command prompt.
2. Using `keytool`, generate a key pair:

```
keytool -genkeypair -keyalg RSA -dname "consumer_dname" -alias orakey
-keypass key_password -keystore keystore -storepass keystore_password
-validity days_valid
```

Where:

- `consumer_dname` is the name of the consumer. This can be any string as long as it's in the correct format (for example, `cn=spaces,dc=example,dc=com`)
- `key_password` is the password for the new public key, (for example, `welcome1`)
- `keystore` is the keystore name, (for example, `default-keystore.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, 1064).

Example 34–1 Generating the Keypair

```
keytool -genkeypair -keyalg RSA -dname "cn=spaces,dc=example,dc=com" -alias orakey
-keypass welcome1 -keystore default-keystore.jks -storepass welcome1 -validity
1064
```

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:

```
keytool -exportcert -v -alias orakey -keystore keystore -storepass
keystore_password -rfc -file orakey.cer
```

Where:

- *keystore* is the keystore name, (for example, `default-keystore.jks`)
- *keystore_password* is the keystore password, (for example, `welcome1`)

Example 34–2 Exporting the Certificate Containing the Public Key

```
keytool -exportcert -v -alias orakey -keystore default-keystore.jks -storepass
welcome1 -rfc -file orakey.cer
```

4. Import the certificate with the alias `webcenter_spaces_ws` (choose **Yes** when prompted whether to overwrite the existing certificate with the alias `orakey`):

```
keytool -importcert -alias webcenter_spaces_ws -file orakey.cer
-keystore default-keystore.jks -storepass keystore_password
```

Where:

- *keystore_password* is the keystore password

Example 34–3 Importing the Certificate

```
keytool -importcert -alias webcenter_spaces_ws -file orakey.cer -keystore
default-keystore.jks -storepass welcome1
```

5. Continue by configuring the keystore using either WLST as described in [Section 34.1.2.2, "Configuring the Keystore with WLST,"](#) or using Fusion Middleware Control as described in [Section 34.1.2.3, "Configuring the Keystore Using Fusion Middleware Control."](#)

[Table 34–2](#) shows the keystore contents you should wind up with after creating and configuring the keystore.

Table 34–2 Portal Domain Keystore Contents for a Simple Topology

Key Alias	Description
orakey	Key pair used to sign and encrypt outbound messages from Spaces. This key is used by both OWSM (Portlets and Worklist) and Discussions.

Table 34–2 (Cont.) Portal Domain Keystore Contents for a Simple Topology

Key Alias	Description
webcenter_spaces_ws	Certificate containing the public key for the <code>orakey</code> private key used in the WebCenter Portal domain. The certificate is used to encrypt outbound WebService messages from the Workflow application on BPEL Server1 in the WebCenter Portal domain, to the WebService APIs on WebCenter Portal domain.

34.1.2.2 Configuring the Keystore with WLST

After creating the keystore, configure the keystore service and update the credential store so that OWSM can read the keystore and keys correctly. You can do this using either Fusion Middleware control, as described in [Section 34.1.2.3, "Configuring the Keystore Using Fusion Middleware Control,"](#) or using WLST as described below.

To configure the credential store:

1. Go to the `<DOMAIN_HOME>/config/fmwconfig` directory, and open the file `jps-config.xml` in an editor.

2. Locate the `<serviceInstance` node for the keystore.provider Provider:

```
<serviceInstance name="keystore" provider="keystore.provider"
location="./default-keystore.jks">
<description>Default JPS Keystore Service</description>
```

3. Make sure that the `default-keystore.jks` keystore file is copied to the `<DOMAIN_HOME>/config/fmwconfig` directory, and that the location is specified as `./default-keystore.jks`:

```
<serviceInstance name="keystore" provider="keystore.provider"
location="./default-keystore.jks">
<description>Default JPS Keystore Service</description>
```

4. Use the following WLST commands to update the credential store:

```
updateCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password=keystore_password, desc="Keystore key")
updateCred(map="oracle.wsm.security", key="enc-csf-key", user="orakey",
password=private_key_password, desc="Encryption key")
updateCred(map="oracle.wsm.security", key="sign-csf-key", user="orakey",
password=private_key_password, desc="Signing key")
```

Where:

- `keystore_password` is the keystore password specified in step 2 of [Section 34.1.2.1, "Creating the WebCenter Portal Domain Keystore,"](#) (for example, `welcome1`)
- `private_key_password` is the private key password specified in step 2 of [Section 34.1.2.1, "Creating the WebCenter Portal Domain Keystore,"](#) (for example, `welcome1`)

Example 34–4 Updating the Credential Store

```
updateCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password="welcome1", desc="Keystore key")
updateCred(map="oracle.wsm.security", key="enc-csf-key", user="orakey",
password="welcome1", desc="Encryption key")
updateCred(map="oracle.wsm.security", key="sign-csf-key", user="orakey",
password="welcome1", desc="Signing key")
```

- Restart all servers.

34.1.2.3 Configuring the Keystore Using Fusion Middleware Control

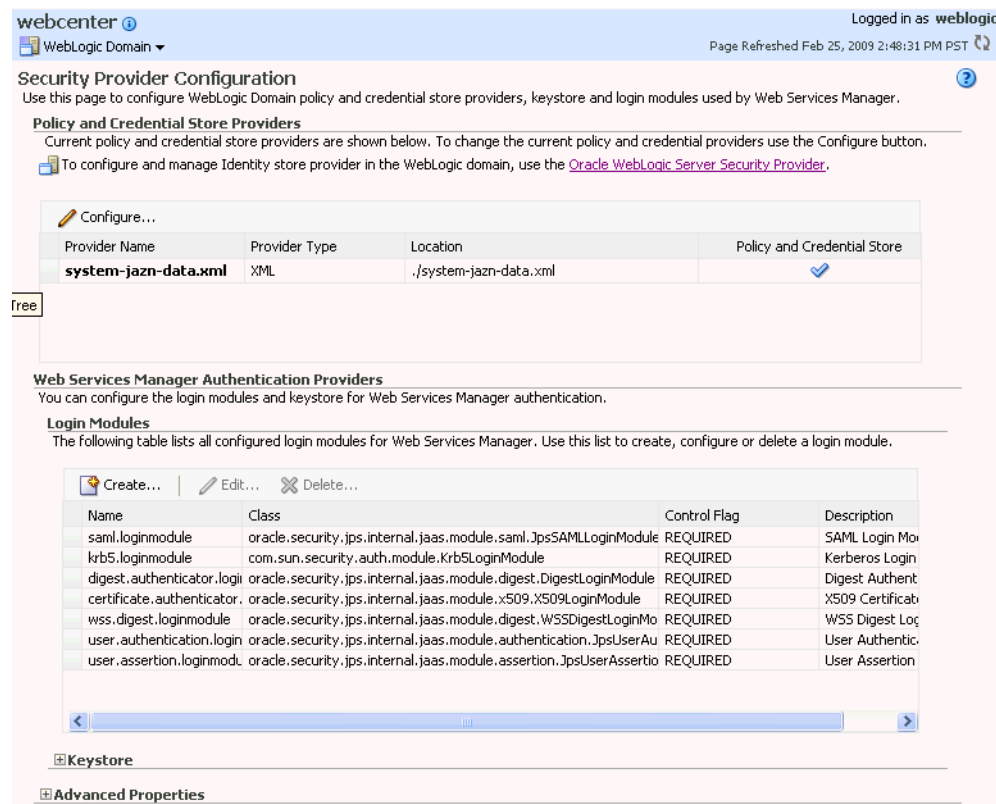
After creating the keystore, configure the keystore service and update the credential store so that OWSM can read the keystore and keys correctly. You can do this using either WLST, as described in [Section 34.1.2.2, "Configuring the Keystore with WLST,"](#) or using Fusion Middleware control as described below.

To configure the keystore provider:

- Ensure that the `default-keystore.jks` keystore file is copied to the `<DOMAIN_HOME>/config/fmwconfig` directory, and then specify the location as `./default-keystore.jks`.
- Open Fusion Middleware Control and log in to the WebCenter Portal domain.
For information on logging in to Fusion Middleware Control, see [Chapter 6, "Starting Enterprise Manager Fusion Middleware Control."](#)
- In the Navigation pane, expand the WebLogic Domain node and click the WebCenter Portal domain (`wc_domain` by default).
- From the WebLogic Domain menu, select **Security -> Security Provider Configuration**.

The Security Provider Configuration page displays (see [Figure 34-3](#)).

Figure 34-3 Security Provider Configuration Page



- Expand the Keystore section on the Security Provider Configuration page.
- Click **Configure**.

The Keystore Configuration page displays (see [Figure 34-4](#)).

Figure 34-4 Keystore Configuration Page

Security Provider Configuration > Configure Key Store

Information
All changes made in this page require a server restart to take effect.

Keystore Configuration OK Cancel

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 will need to provide the keystore name, path, password and information about default identity certificates.

Keystore Type:

Access Attributes

* 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" value="orakey"/>	* Crypt Alias: <input type="text" value="orakey"/>
* Signature Password: <input type="password" value="....."/>	* Crypt Password: <input type="password" value="....."/>
* Confirm Password: <input type="password" value="....."/>	* Confirm Password: <input type="password" value="....."/>

7. Use the following settings to specify the location of the keystore that contains the certificate and private key, and the signature key and encryption key aliases:
 - **Keystore Path:** ./default-keystore.jks
 - **Password:** Enter and confirm the password for the keystore.
 - **Key Alias:** orakey
 - **Signature Password:** Enter and confirm the password for the signature key.
 - **Crypt Alias:** orakey
 - **Crypt Password:** Enter and confirm the password for the encryption key.
8. Click **OK** to save your settings.
9. Restart the Administration server for the domain.

34.1.3 Configuring the Discussions Server for a Simple Topology

In a simple topology, the discussions server is in the same domain as Spaces and consequently no extra keystore configuration is needed since the keystore configured for the WebCenter Portal domain is used for the Discussions service as well. However, for production environments you should protect the Discussion service Web Service end points with an OWSM policy and configure the discussions server connection settings. These configuration steps are described in the following subsections:

- [Section 34.1.3.1, "Securing the Discussions Service End Points"](#)
- [Section 34.1.3.2, "Configuring the Discussions Server Connection Settings"](#)

Note: Discussions-specific Web Services messages sent by WebCenter Portal applications to the Oracle WebCenter Portal's Discussions server are not encrypted. For message confidentiality, the discussions server URL must be accessed over Secure Socket Layer (SSL). For more information, see [Chapter 33, "Configuring SSL."](#)

34.1.3.1 Securing the Discussions Service End Points

The WebCenter Portal's Discussions service's Web Service end points require user identity to be propagated for calls originating from Spaces. Out-of-the-box, the Discussions service Web Service end points are configured with a policy that uses an unsecured SAML token to let you get up and running in a test environment without having to fully implement security. For a production environment, however, the Web Service end points need to be secured with OWSM policies to ensure that messages are not tampered with, and can't be viewed by others while in transit. To do this, both the public access WebService end point and authenticated user access end point should be secured with the appropriate OWSM policies using either Fusion Middleware Control or WLST.

This section contains the following subsections:

- [Section 34.1.3.1.1, "Securing the Discussions Server End Points Using Fusion Middleware Control"](#)
- [Section 34.1.3.1.2, "Securing the Discussions Server End Points Using WLST"](#)

34.1.3.1.1 Securing the Discussions Server End Points Using Fusion Middleware Control

To secure the Discussions service end points using Fusion Middleware Control, follow the steps below:

1. Log in to Fusion Middleware Control and from the Navigation pane, expand **WebCenter> Portal> Discussions** and click Discussions (WC_Collaboration).

The Discussions home page displays (see [Figure 34-5](#)).

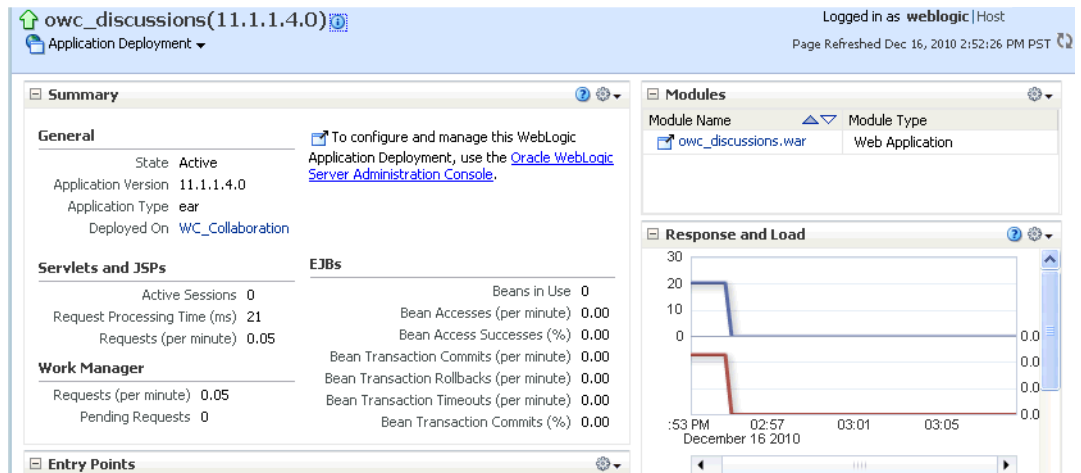
Figure 34-5 Discussions Home Page



2. Click the owc_discussions target.

The home page for the owc_discussions application displays (see [Figure 34-6](#)).

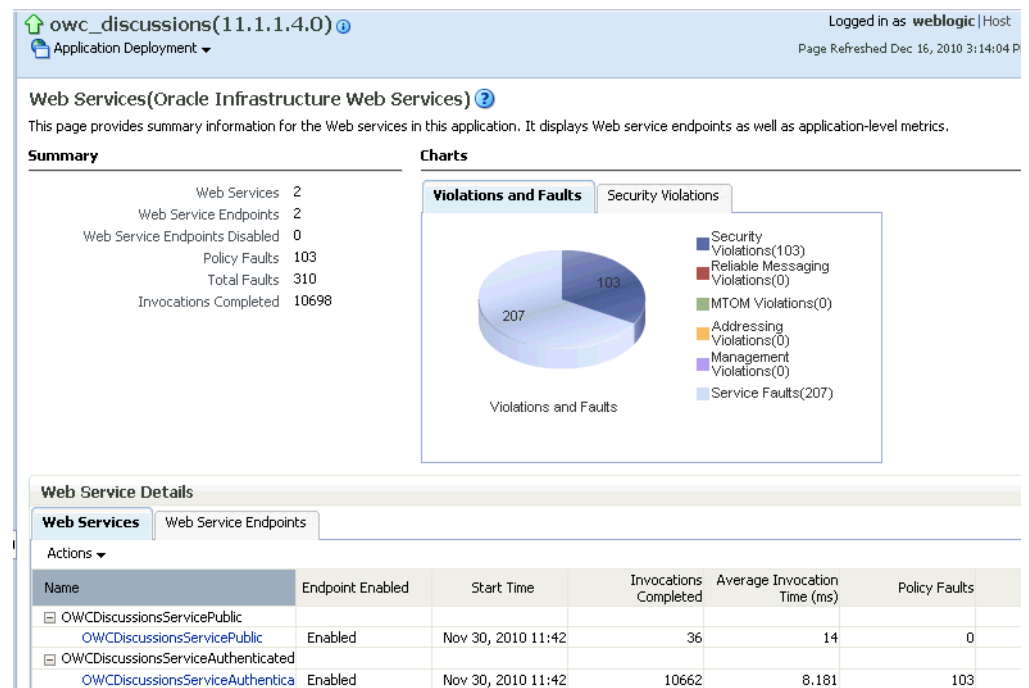
Figure 34–6 *owc_discussions Home Page*



- From the Application Deployment menu, select **Web Services**.

The Web Services page for the `owc_discussions` application displays (see Figure 34–7).

Figure 34–7 *Web Services Page for owc_discussions*



- Open the Web Services tab, and click the `OWCDiscussionsServiceAuthenticated` Web Service end point.

The Web Service Endpoint page for `owc_discussions` displays (see Figure 34–8).

Figure 34–8 Web Service Endpoint Page

owc_discussions(11.1.1.4.0) Application Deployment Logged in as weblogic|Host Page Refreshed Dec 16, 2010 3:21:52 PM PST

Web Services > Web Service Endpoint

OWCDiscussionsServiceAuthenticated (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
Asynchronous	False	Data Binding	jaxb20
Style	document	Legacy Configuration	False
SOAP Version	soap1.1	Implementation Class	oracle.jive.webservice.server.OWCDiscussionsServiceAuthenticated
Stateful	False	WSDL Document	OWCDiscussionsServiceAuthenticated
Implementation Type	JAX-WS		

Operations | **OWSM Policies** | Charts | Configuration

Globally Attached Policies

Policy Name	Policy Set	Category	Total Violations	Security Violations	
				Authentication	Authorization
No rows yet					

Directly Attached Policies

Attach/Detach

Policy Name	Category	Policy Reference Status	Total Violations	Security Violations		Con
				Authentication	Authorization	
oracle/wss10_saml_token_service_policy	Security	Enabled	103	0	0	

5. Click Attach/Detach.

The Attach Policy page displays (see [Figure 34–9](#)).

Figure 34–9 Attach Policy Page

owc_discussions(11.1.1.4.0) | Logged in as weblogic | Host
 Application Deployment | Page Refreshed Dec 16, 2010 3:28:20 PM PST

Web Services > Web Service Endpoint > Attach Policies

Attach/Detach Policies(OWCDiscussionsServiceAuthenticated) [OK] [Validate] [Cancel]

Globally Attached Policies

Name	Policy Set	Category	Enabled	Description
No rows yet				

Directly Attached Policies

Name	Category	Enabled	Description	View Detail
oracle/wss10_saml_token_service_policy	Security	✓	This policy authenticates ...	🔗

[Attach] [Detach]

Available Policies

Name	Category	Enabled	Description	View Detail
oracle/wss11_message_protection_service_policy	Security	✓	This policy enforces messa...	🔗
oracle/wss11_saml20_token_with_message_protection_service_policy	Security	✓	This policy enforces messa...	🔗
oracle/wss11_saml_or_username_token_with_message_protection_service_policy	Security	✓	This policy enforces messa...	🔗
oracle/wss11_saml_token_with_message_protection_service_policy	Security	✓	This policy enforces messa...	🔗
oracle/wss11_sts_issued_saml_hok_with_message_protection_service_policy	Security	✓	This policy authenticates ...	🔗
oracle/wss11_username_token_with_message_protection_service_policy	Security	✓	This policy enforces messa...	🔗
oracle/wss11_x509_token_with_message_protection_service_policy	Security	✓	This policy enforces messa...	🔗
oracle/wss_http_token_over_ssl_service_policy	Security	✓	This policy extracts the c...	🔗
oracle/wss_http_token_service_policy	Security	✓	This policy uses the crede...	🔗
oracle/wss_saml20_token_bearer_over_ssl_service_policy	Security	✓	This policy authenticates ...	🔗
oracle/wss_saml20_token_over_ssl_service_policy	Security	✓	This policy authenticates ...	🔗

6. Use the **Attach** and **Detach** buttons to attach `oracle/wss11_saml_token_with_message_protection_service_policy` and detach `oracle/wss10_saml_token_service_policy`.
7. Click **OK**.
8. Return to the Web Services page and click the `OWCDiscussionsServicePublic` end point.
9. Attach `oracle/wss11_message_protection_service_policy` so that the public user Web Service end point is also secured.
10. Click **OK**.

34.1.3.1.2 Securing the Discussions Server End Points Using WLST

To secure the discussions server end points using WLST, detach the `wss10_saml_token_service_policy` and attach the `wss11_saml_token_with_message_protection_service_policy` using the following WLST commands:

```
detachWebServicePolicy('owc_discussions', 'owc_discussions', 'web',
'OWCDiscussionsServiceAuthenticated', 'OWCDiscussionsServiceAuthenticated',
'oracle/wss10_saml_token_service_policy')
attachWebServicePolicy('owc_discussions', 'owc_discussions', 'web',
'OWCDiscussionsServiceAuthenticated', 'OWCDiscussionsServiceAuthenticated',
'oracle/wss11_saml_token_with_message_protection_service_policy')
```

34.1.3.2 Configuring the Discussions Server Connection Settings

You must supply the WS-Security client certificate information within the discussions server connection that is configured for Spaces or your WebCenter Portal application, as described in [Section 14.3, "Registering Discussions Servers."](#) [Figure 34–10](#) shows example connection detail settings for the Edit Discussions and Announcement Connection page.

Figure 34–10 Edit Discussions and Announcement Connection Page

Edit Discussion and Announcement Connection ?

Name

Connection Name JiveCn

Active Connection

Connection Details

* Server URL

* Administrator User Name

Authenticated User WebService Policy URI

Public User WebService Policy URI

* Recipient Key Alias

Advanced Configuration

Specify additional (optional) configuration properties for the connection.

Connection Timeout (seconds)

Additional Properties

Enter names and values for any additional properties.

Property Name	Property Value	Is Property Secured?
No Data Available		

34.1.4 Command Summary for a Simple Topology

Use the following command summary to quickly configure the keystore for a simple topology.

Generate the Keystore

Use the following `keytool` commands to generate the keystore, replacing the values in bold with those for your local environment:

```
keytool -genkeypair -keyalg RSA -dname "cn=spaces, dc=example, dc=com" -alias orakey
-keypass welcome1 -keystore default-keystore.jks -storepass welcome1 -validity
1064
```

```
keytool -exportcert -v -alias orakey -keystore default-keystore.jks -storepass
welcome1 -rfc -file orakey.cer
```

```
keytool -importcert -alias webcenter_spaces_ws -file orakey.cer
-keystore default-keystore.jks -storepass welcome1
```

When prompted that the certificate already exists, say `yes`.

```
keytool -importcert -alias df_orakey_public -file orakey.cer
-keystore owc_discussions.jks -storepass welcome1
```

Copy the `default-keystore.jks` file to your `domain_home/config/fmwconfig` directory.

Configure the Keystore

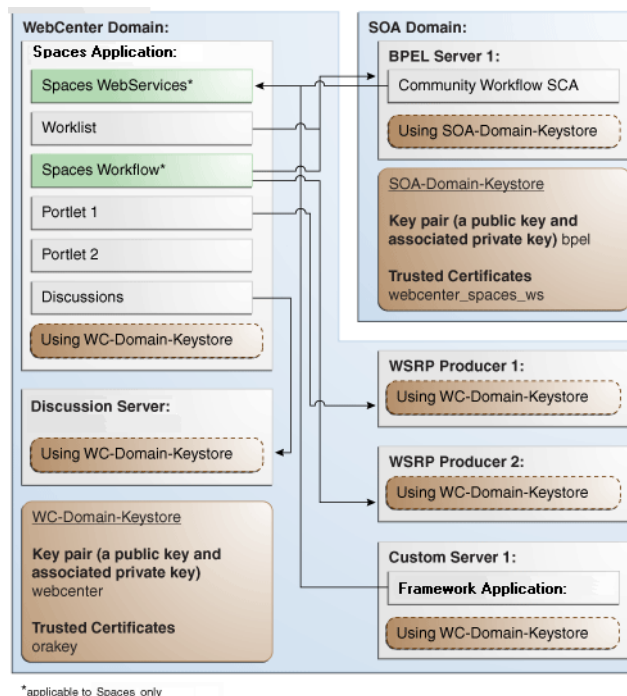
Using WLST, connect to the Spaces domain as an administrator and run the following commands:

```
updateCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password="welcome1", desc="Keystore key")
updateCred(map="oracle.wsm.security", key="enc-csf-key", user="orakey",
password="welcome1", desc="Encryption key")
updateCred(map="oracle.wsm.security", key="sign-csf-key", user="orakey",
password="welcome1", desc="Signing key")
```

34.2 Configuring WS-Security for a Typical Topology

This section describes how to configure WS-Security for a topology where the WebCenter Portal application and the WSRP producers share the same domain, but the BPEL server is in an external domain - the SOA domain (see [Figure 34-11](#)).

Figure 34-11 WS-Security for a Typical Configuration



The steps to configure WS-Security for a typical two domain WebCenter Portal topology are described in the following sections:

- [Section 34.2.1, "Roadmap to Configuring WS-Security for a Typical Topology"](#)
- [Section 34.2.2, "Setting Up the WebCenter Portal Domain Keystore"](#)
- [Section 34.2.3, "Configuring the Discussions Server for a Typical Topology"](#)
- [Section 34.2.4, "Setting Up the SOA Domain"](#)
- [Section 34.2.5, "Command Summary for a Typical Topology"](#)

34.2.1 Roadmap to Configuring WS-Security for a Typical Topology

The flow chart (Figure 34–12) and table (Table 34–3) in this section provide an overview of the prerequisites and tasks required to configure WS-Security for a typical WebCenter Portal topology.

Figure 34–12 Configuring WS-Security for a Typical Topology

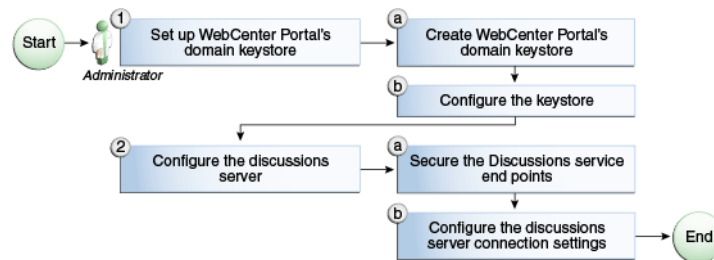


Table 34–3 shows the tasks and sub-tasks to configure WS-Security for a typical WebCenter Portal topology.

Table 34–3 Configuring WS-Security for a Typical Topology

Actor	Task	Sub-task	Notes
Administrator	1. Set up the WebCenter Portal domain keystore	1.a Create the WebCenter Portal domain keystore 1.b Configure the keystore	
	2. Configure the discussions server	2.a Secure the Discussions service end points 2.b Configure the discussions server connection settings	

34.2.2 Setting Up the WebCenter Portal Domain Keystore

The security credentials of a WebCenter Portal application, discussions server, BPEL server (in a separate domain), and WSRP producers 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.

This section contains the following subsections:

- [Section 34.2.2.1, "Creating the WebCenter Portal Domain Keystore"](#)
- [Section 34.2.2.2, "Configuring the Keystore Using WLST"](#)
- [Section 34.2.2.3, "Configuring the Keystore Using Fusion Middleware Control"](#)

34.2.2.1 Creating the WebCenter Portal Domain Keystore

This section describes how to create a keystore 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 the WebCenter Portal domain keystore:

1. Go to `JDK_HOME/jdk/bin` and open a command prompt.

2. Using keytool, generate a key pair:

```
keytool -genkeypair -keyalg RSA -dname "consumer_dname" -alias webcenter
-keypass key_password -keystore keystore -storepass keystore_password -validity
days_valid
```

Where:

- *consumer_dname* is the name of the consumer (for example, `cn=spaces,dc=example,dc=com`)
- *key_password* is the password for the new public key, (for example, `welcome1`)
- *keystore* is the keystore name, (for example, `webcenter.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, `1064`).

Example 34-5 Generating the Keypair

```
keytool -genkeypair -keyalg RSA -dname "cn=spaces,dc=example,dc=com" -alias
webcenter -keypass welcome1 -keystore webcenter.jks -storepass welcome1
-validity 1064
```

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:

```
keytool -exportcert -v -alias webcenter -keystore keystore
-storepass keystore_password -rfc -file webcenter_public.cer
```

Where:

- *keystore* is the keystore name, (for example, `webcenter.jks`)
- *keystore_password* is the keystore password, (for example, `welcome1`)

Example 34-6 Exporting the Certificate Containing the Public Key

```
keytool -exportcert -v -alias webcenter -keystore webcenter.jks
-storepass welcome1 -rfc -file webcenter_public.cer
```

4. Continue by configuring the keystore using either WLST, as described in [Section 34.2.2.2, "Configuring the Keystore Using WLST,"](#) or Fusion Middleware Control, as described in [Section 34.2.2.3, "Configuring the Keystore Using Fusion Middleware Control."](#)

[Table 34-4](#) shows the keystore contents you should wind up with after creating and configuring the keystore.

Table 34–4 WebCenter Portal Domain Keystore Contents for a Typical Topology

Key Alias	Description
webcenter	Key pair used to sign and encrypt outbound messages from Spaces. This key is used by both OWSM (Portlets and Worklist) and Discussions.
orakey	Certificate containing the public key for the BPEL private key used in the SOA domain. The certificate is used to encrypt outbound WebService messages from the Workflow application on BPEL Server1 in the WebCenter Portal domain, to the Worklist service to the SOA server on the SOA domain.

34.2.2.2 Configuring the Keystore Using WLST

After creating the WebCenter Portal domain keystore, configure the keystore service and update the credential store so that OWSM can read the keystore and keys correctly. You can do this either using Fusion Middleware Control, as described in [Section 34.2.2.3, "Configuring the Keystore Using Fusion Middleware Control,"](#) or using WLST as described below.

To configure the keystore service:

1. Go to the `<DOMAIN_HOME>/config/fmwconfig` directory, and open the file `jps-config.xml` in an editor.
2. Locate the `<serviceInstance` node for the `keystore.provider Provider`
3. Ensure that the `webcenter.jks` keystore file is copied to the `<DOMAIN_HOME>/config/fmwconfig` directory, and then specify the location as `./webcenter.jks`.
4. Use the following WLST commands to update the credential store:

```
updateCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password=keystore_password, desc="Keystore key")
updateCred(map="oracle.wsm.security", key="enc-csf-key", user="webcenter",
password=private_key_password, desc="Encryption key")
updateCred(map="oracle.wsm.security", key="sign-csf-key", user="webcenter",
password=private_key_password, desc="Signing key")
```

Where:

- `keystore_password` is the keystore password specified in step 2 of [Section 34.2.2.1, "Creating the WebCenter Portal Domain Keystore,"](#) (for example, `welcome1`)
- `private_key_password` is the private key password specified in step 2 of [Section 34.2.2.1, "Creating the WebCenter Portal Domain Keystore,"](#) (for example, `welcome1`)

Example 34–7 Updating the Credential Store

```
updateCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password="welcome1", desc="Keystore key")
updateCred(map="oracle.wsm.security", key="enc-csf-key", user="webcenter",
password="welcome1", desc="Encryption key")
updateCred(map="oracle.wsm.security", key="sign-csf-key", user="webcenter",
password="welcome1", desc="Signing key")
```

5. Restart all servers.

34.2.2.3 Configuring the Keystore Using Fusion Middleware Control

After creating the keystore, configure the keystore service and update the credential store so that OWSM can read the keystore and keys correctly. You can do this either using WLST, as described in [Section 34.2.2.2, "Configuring the Keystore Using WLST,"](#) or using Fusion Middleware Control as described below.

To configure the keystore provider:

1. Open Fusion Middleware Control and log in to the WebCenter Portal domain.
For information on logging in to Fusion Middleware Control, see [Chapter 6, "Starting Enterprise Manager Fusion Middleware Control."](#)
2. In the Navigation pane, expand the WebLogic Domain node and click the WebCenter Portal domain (`wc_domain` by default).
3. From the WebLogic Domain menu, select **Security -> Security Provider Configuration**.

The Security Provider Configuration page displays (see [Figure 34–13](#)).

Figure 34–13 Security Provider Configuration Page

The screenshot shows the 'Security Provider Configuration' page. At the top, it says 'webcenter' and 'Logged in as weblogic'. Below that, it says 'WebLogic Domain' and 'Page Refreshed Feb 25, 2009 2:48:31 PM PST'. The main heading is 'Security Provider Configuration' with a sub-heading 'Use this page to configure WebLogic Domain policy and credential store providers, keystore and login modules used by Web Services Manager.' There are two sections: 'Policy and Credential Store Providers' and 'Web Services Manager Authentication Providers'. The 'Policy and Credential Store Providers' section has a 'Configure...' button and a table with columns: Provider Name, Provider Type, Location, and Policy and Credential Store. The table has one row: 'system-jazn-data.xml', 'XML', './system-jazn-data.xml', and a checkmark. The 'Web Services Manager Authentication Providers' section has a 'Login Modules' sub-section with a table listing login modules. The table has columns: Name, Class, Control Flag, and Description. The table has six rows: 'saml.loginmodule', 'krb5.loginmodule', 'digest.authenticator.loginmodule', 'certificate.authenticator', 'wss.digest.loginmodule', and 'user.authentication.loginmodule'. Each row has a 'Create...', 'Edit...', and 'Delete...' button above it.

Provider Name	Provider Type	Location	Policy and Credential Store
system-jazn-data.xml	XML	./system-jazn-data.xml	<input checked="" type="checkbox"/>

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.loginmodule	oracle.security.jps.internal.jaas.module.digest.DigestLoginModule	REQUIRED	Digest Authent
certificate.authenticator	oracle.security.jps.internal.jaas.module.x509.X509LoginModule	REQUIRED	X509 Certificat
wss.digest.loginmodule	oracle.security.jps.internal.jaas.module.digest.WSSDigestLoginMo	REQUIRED	WSS Digest Lo
user.authentication.loginmodule	oracle.security.jps.internal.jaas.module.authentication.JpsUserAu	REQUIRED	User Authentic
user.assertion.loginmodule	oracle.security.jps.internal.jaas.module.assertion.JpsUserAssertio	REQUIRED	User Assertion

4. Expand the Keystore section on the Security Provider Configuration page.
5. Click **Configure**.

The Keystore Configuration page displays (see [Figure 34–14](#)).

Figure 34–14 Keystore Configuration Page

Security Provider Configuration > Configure Key Store

Information
All changes made in this page require a server restart to take effect.

Keystore Configuration OK Cancel

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 will need to provide the keystore name, path, password and information about default identity certificates.

Keystore Type:

Access Attributes

* 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.

<p>Signature Key</p> <p>* Key Alias: <input type="text" value="webcenter"/></p> <p>* Signature Password: <input type="password" value="....."/></p> <p>* Confirm Password: <input type="password" value="....."/></p>	<p>Encryption Key</p> <p>* Crypt Alias: <input type="text" value="webcenter"/></p> <p>* Crypt Password: <input type="password" value="....."/></p> <p>* Confirm Password: <input type="password" value="....."/></p>
--	---

6. Use the following settings to specify the location of the keystore that contains the certificate and private key, and the signature key and encryption key aliases:
 - **Keystore Path:** `./webcenter.jks`
 - **Password:** Enter and confirm the password for the keystore.
 - **Key Alias:** `webcenter`
 - **Signature Password:** Enter and confirm the password for the signature key.
 - **Crypt Alias:** `webcenter`
 - **Crypt Password:** Enter and confirm the password for the encryption key.
7. Click **OK** to save your settings.
8. Restart the Administration server for the domain.

34.2.3 Configuring the Discussions Server for a Typical Topology

Configuring the discussions server for a typical topology is exactly the same as for a simple topology. For more information, see [Section 34.1.3, "Configuring the Discussions Server for a Simple Topology."](#)

34.2.4 Setting Up the SOA Domain

This section describes how to set up the SOA domain keystore and contains the following subsections:

- [Section 34.2.4.1, "Creating the SOA Domain Keystore"](#)
- [Section 34.2.4.2, "Configuring the Keystore Using WLST"](#)
- [Section 34.2.4.3, "Configuring the Keystore Using Fusion Middleware Control"](#)

34.2.4.1 Creating the SOA Domain Keystore

This section describes how to create a SOA domain keystore and keys using a Java Keystore (JKS).

To create the SOA domain keystore:

1. Go to `JDK_HOME/jdk/bin` and open a command prompt.

2. Create a keystore by importing the public certificate (`webcenter_public.cer`) from the WebCenter Portal domain:

```
keytool -importcert -alias webcenter_spaces_ws -file webcenter_public.cer
-keystore bpel.jks -storepass keystore_password
```

Where:

- `keystore_password` is the keystore password, (for example, `welcome1`)

Example 34–8 Importing the Public Certificate

```
keytool -importcert -alias webcenter_spaces_ws -file webcenter_public.cer
-keystore bpel.jks -storepass welcome1
```

3. Using `keytool`, create a keypair to be used in the SOA domain for signing and encrypting messages:

```
keytool -genkeypair -keyalg RSA -dname "consumer_dname" -alias bpel
-keypass key_password -keystore keystore -storepass keystore_password
-validity days_valid
```

Where:

- `consumer_dname` is the name of the consumer (for example, `cn=bpel,dc=example,dc=com`)
- `key_password` is the password for the new public key, (for example, `welcome1`)
- `keystore` is the keystore name, (for example, `bpel.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, `1064`).

Example 34–9 Generating the Keypair

```
keytool -genkeypair -keyalg RSA -dname "cn=bpel,dc=example,dc=com" -alias bpel
-keypass welcome1 -keystore bpel.jks -storepass welcome1 -validity 1064
```

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.

4. Export the certificate so it can be imported in the WebCenter Portal domain using the `orakey` alias:

```
keytool -exportcert -v -alias bpel -keystore keystore -storepass
keystore_password -rfc -file orakey.cer
```

Where:

- `keystore` is the keystore name, (for example, `webcenter.jks`)
- `keystore_password` is the keystore password, (for example, `welcome1`)

Example 34–10 Exporting the Certificate Containing the Public Key

```
keytool -exportcert -v -alias bpel -keystore bpel.jks -storepass welcome1 -rfc
```

```
-file orakay.cer
```

5. Import the certificate with a different alias (choose **Yes** when prompted whether to overwrite the existing certificate with the alias `orakey`):

```
keytool -importcert -alias orakey -file orakey.cer -keystore webcenter.jks
-storepass keystore_password
```

Where:

- `keystore_password` is the keystore password

Example 34–11 Importing the Certificate

```
keytool -importcert -alias orakey -file orakay.cer -keystore webcenter.jks
-storepass welcome1
```

34.2.4.2 Configuring the Keystore Using WLST

After creating the SOA domain keystore, configure the keystore service and update the credential store so that OWSM can read the keystore and keys correctly. You can do this either with Fusion Middleware Control, as described in [Section 34.2.4.3, "Configuring the Keystore Using Fusion Middleware Control,"](#) or using WLST as described below.

To configure the keystore service:

1. Go to the `<DOMAIN_HOME>/config/fmwconfig` directory, and open the file `jps-config.xml` in an editor.
2. Locate the `<serviceInstance` node for the `keystore.provider Provider`
3. Ensure that the `bpel.jks` keystore file is copied to the `<DOMAIN_HOME>/config/fmwconfig` directory, and then specify the location as `./bpel.jks`.
4. Use the following WLST commands to configure the credential store:

```
updateCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password="welcome1", desc="Keystore key")
updateCred(map="oracle.wsm.security", key="enc-csf-key", user="bpel",
password="welcome1", desc="Encryption key")
updateCred(map="oracle.wsm.security", key="sign-csf-key", user="bpel",
password="welcome1", desc="Signing key")
```

5. Restart all servers.

34.2.4.3 Configuring the Keystore Using Fusion Middleware Control

After creating the keystore, configure the keystore service and update the credential store so that OWSM can read the keystore and keys correctly. You can do this either with WLST, as described in [Section 34.2.4.2, "Configuring the Keystore Using WLST,"](#) or using Fusion Middleware Control as described below.

To configure the keystore provider:

1. Open Fusion Middleware Control and log in to the SOA domain.
For information on logging in to Fusion Middleware Control, see [Chapter 6, "Starting Enterprise Manager Fusion Middleware Control."](#)
2. In the Navigation pane, expand the WebLogic Domain node and click the SOA domain.

3. From the WebLogic Domain menu, select **Security -> Security Provider Configuration**.
4. Expand the Keystore section on the Security Provider Configuration page.
5. Click **Configure**.

The Keystore Configuration page displays (see [Figure 34–15](#)).

Figure 34–15 Keystore Configuration Page

Security Provider Configuration > Configure Key Store

Information
All changes made in this page require a server restart to take effect.

Keystore Configuration OK Cancel

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 will need to provide the keystore name, path, password and information about default identity certificates.

Keystore Type

Access Attributes

* 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.

<p>Signature Key</p> <p>* Key Alias <input type="text" value="bpel"/></p> <p>* Signature Password <input type="password" value="....."/></p> <p>* Confirm Password <input type="password" value="....."/></p>	<p>Encryption Key</p> <p>* Crypt Alias <input type="text" value="bpel"/></p> <p>* Crypt Password <input type="password" value="....."/></p> <p>* Confirm Password <input type="password" value="....."/></p>
--	---

6. Use the following settings to specify the location of the keystore that contains the certificate and private key, and the signature key and encryption key aliases:
 - **Keystore Path:** `./bpel.jks`
 - **Password:** Enter and confirm the password for the keystore.
 - **Key Alias:** `bpel`
 - **Signature Password:** Enter and confirm the password for the signature key.
 - **Crypt Alias:** `bpel`
 - **Crypt Password:** Enter and confirm the password for the encryption key.
7. Click **OK** to save your settings.
8. Restart the Administration server for the domain.

34.2.5 Command Summary for a Typical Topology

Use the following command summary to quickly configure the keystore for a typical topology.

Generate the Keystore

Use the following `keytool` commands to generate the keystore, replacing the values in bold with those for your local environment:

```
keytool -genkeypair -keyalg RSA -dname "cn=spaces,dc=example,dc=com" -alias
webcenter -keypass welcome1 -keystore webcenter.jks -storepass welcome1 -validity
1064
```

```
keytool -exportcert -v -alias webcenter -keystore webcenter.jks
```

```
-storepass welcome1 -rfc -file webcenter_public.cer
```

```
keytool -importcert -alias webcenter_spaces_ws -file webcenter_public.cer
-keystore bpel.jks -storepass welcome1
```

When prompted that the certificate already exists, say yes.

```
keytool -genkeypair -keyalg RSA -dname "cn=bpel,dc=example,dc=com" -alias bpel
-keypass welcome1 -keystore bpel.jks -storepass welcome1 -validity 1024
```

```
keytool -exportcert -v -alias bpel -keystore bpel.jks -storepass welcome1
-rfc -file orakay.cer
```

```
keytool -importcert -alias orakey -file orakay.cer -keystore webcenter.jks
-storepass welcome1
```

When prompted to trust the certificate, say yes.

```
keytool -importcert -alias df_webcenter_public -file webcenter_public.cer
-keystore owc_discussions.jks -storepass welcome1
```

When prompted to trust the certificate, say yes.

Copy the `webcenter.jks` file to your `domain_home/config/fmwconfig` directory, and the `bpel.jks` file to your `soa_domain_home/config/fmwconfig` directory.

Configure the WebCenter Portal Domain Keystore

Follow the steps below to configure the service instance reference for the WebCenter Portal domain:

1. Navigate to the `<DOMAIN_HOME>/config/fmwconfig` directory.
2. Copy `webcenter.jks` to the `<DOMAIN_HOME>/config/fmwconfig` directory if you haven't already done so.
3. Open `jps-config.xml` in an editor.
4. Locate `<serviceInstance` node for `keystore.provider Provider`.
5. Specify the location as `./webcenter.jks`.
6. Using WLST, connect to the Spaces domain as an admin user and run the following commands:

```
updateCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password="welcome1", desc="Keystore key")
updateCred(map="oracle.wsm.security", key="enc-csf-key", user="webcenter",
password="welcome1", desc="Encryption key")
updateCred(map="oracle.wsm.security", key="sign-csf-key", user="webcenter",
password="welcome1", desc="Signing key")
```

Configure the SOA Domain Keystore

Follow the steps below to configure service instance reference for the SOA domain:

1. Navigate to the `<SOA_DOMAIN_HOME>/config/fmwconfig` directory.
2. Copy `bpel.jks` to the `<SOA_DOMAIN_HOME>/config/fmwconfig` directory if you haven't done already done so.
3. Open `jps-config.xml` in an editor.
4. Locate `<serviceInstance` node for `keystore.provider Provider`.
5. Specify the location as `./bpel.jks`.

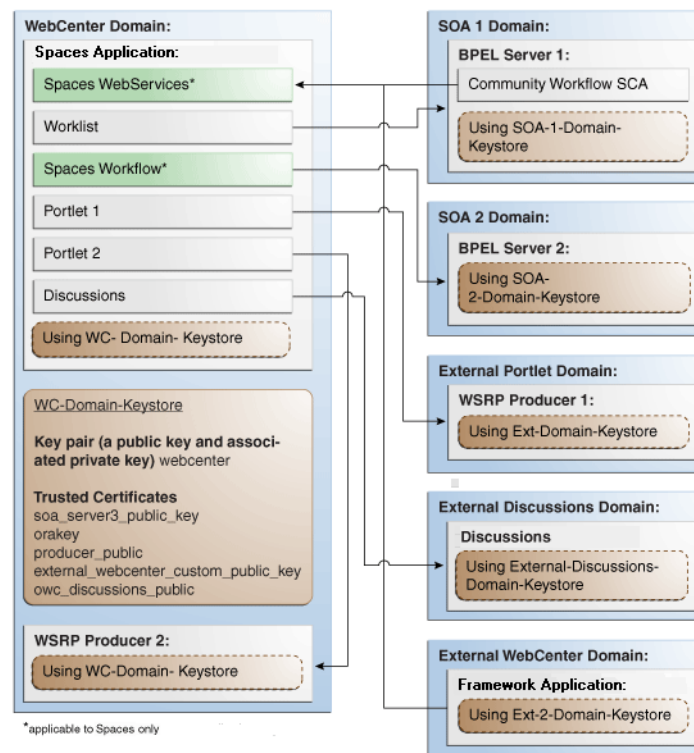
6. Using WLST, connect to the SOA domain as an admin user and run the following commands:

```
updateCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password="welcome1", desc="Keystore key")
updateCred(map="oracle.wsm.security", key="enc-csf-key", user="bpel",
password="welcome1", desc="Encryption key")
updateCred(map="oracle.wsm.security", key="sign-csf-key", user="bpel",
password="welcome1", desc="Signing key")
```

34.3 Configuring WS-Security for a Complex Topology

This section describes how to configure WS-Security for a complex topology where the WebCenter Portal application, the discussions server (Jive), and a WSRP producer are in the same domain, two BPEL servers are in separate SOA domains, and one WSRP producer is in an external portlet domain (see [Figure 34-16](#)).

Figure 34-16 WS-Security for a Complex Configuration



The steps to configure WS-Security for a complex WebCenter Portal topology with multiple domains are described in the following sections:

- [Section 34.3.1, "Roadmap to Configuring WS-Security for a Complex Topology"](#)
- [Section 34.3.2, "Setting Up the WebCenter Portal Domain Keystores"](#)
- [Section 34.3.3, "Configuring the Discussions Server for a Complex Topology"](#)
- [Section 34.3.4, "Setting Up the First SOA Domain"](#)
- [Section 34.3.5, "Setting Up the Second SOA Domain"](#)
- [Section 34.3.6, "Setting Up the External Portlet Domain Keystore"](#)
- [Section 34.3.7, "Setting Up the External WebCenter Portal Domain Keystore"](#)

- Section 34.3.8, "Command Summary for a Complex Topology"

34.3.1 Roadmap to Configuring WS-Security for a Complex Topology

The flow chart (Figure 34-17) and table (Table 34-5) in this section provide an overview of the prerequisites and tasks required to configure WS-Security for a complex multiple-domain WebCenter Portal topology.

Figure 34-17 Configuring WS-Security for a Complex Topology

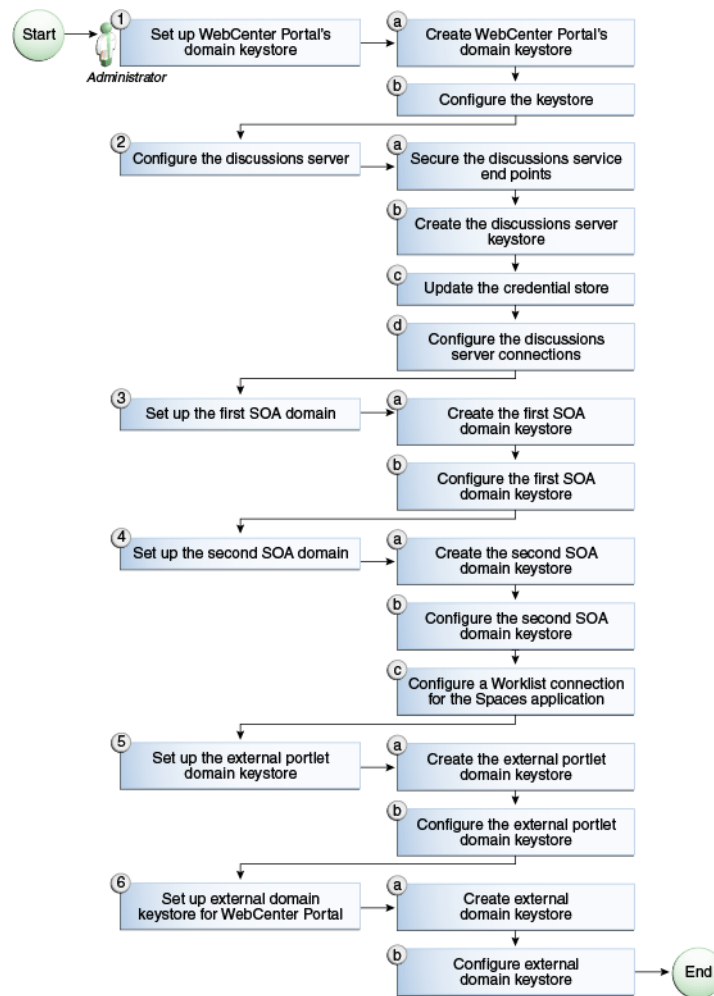


Table 34-5 shows the tasks and sub-tasks to configure WS-Security for a complex WebCenter Portal topology.

Table 34-5 Configuring WS-Security for a Complex Topology

Actor	Task	Sub-task	Notes
Administrator	1. Set up the WebCenter Portal domain keystore	1.a Create the WebCenter Portal domain keystore	
		1.b Configure the keystore	
	2. Configure the discussions server	2.a Secure the Discussions service end points	
		2.b Create the discussions server keystore	
		2.c Update the credential store	
		2.d Configure the discussions server connections	

Table 34–5 (Cont.) Configuring WS-Security for a Complex Topology

Actor	Task	Sub-task	Notes
		2.c Update the credential store	
		2.d Configure the discussions server connections	
	3. Set up the first SOA domain	3.a Create the first SOA domain keystore	
		3.b Configure the first SOA domain keystore	
	4. Set up the second SOA domain	4.a Create the second SOA domain keystore	
		4.b Configure the second SOA domain keystore	
		4.c Configure the Spaces Worklist connection	
	5. Set up the external portlet domain keystore	5.a Create the external portlet domain keystore	
		5.b Configure the external portlet domain keystore	
	6. Set up the external WebCenter Portal domain keystore	6.a Create the external WebCenter Portal domain keystore	
		6.b Configure external WebCenter Portal domain keystore	

34.3.2 Setting Up the WebCenter Portal Domain Keystores

The security credentials of Spaces, discussions server, BPEL servers (in separate domains), and WSRP producers (also in separate domains) 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.

This section contains the following subsections:

- [Section 34.3.2.1, "Creating the WebCenter Portal Domain Keystores"](#)
- [Section 34.3.2.2, "Configuring the Keystore Using WLST"](#)
- [Section 34.3.2.3, "Configuring the Keystore Using Fusion Middleware Control"](#)

34.3.2.1 Creating the WebCenter Portal Domain Keystores

This section describes how to create the 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 the WebCenter Portal domain keystores:

1. Go to `JDK_HOME/jdk/bin` and open a command prompt.
2. Using `keytool`, generate a key pair for the `webcenter` keystore:

```
keytool -genkeypair -keyalg RSA -dname "consumer_dname" -alias webcenter
-keypass key_password -keystore keystore -storepass keystore_password -validity
days_valid
```

Where:

- *consumer_dname* is the name of the consumer (for example, `cn=spaces,dc=example,dc=com`)
- *key_password* is the password for the new public key, (for example, `welcome1`)
- *keystore* is the keystore name, (for example, `webcenter.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, `1064`).

Example 34–12 Generating the Keypair

```
keytool -genkeypair -keyalg RSA -dname "cn=spaces,dc=example,dc=com" -alias  
webcenter -keypass welcome1 -keystore webcenter.jks -storepass welcome1 -validity  
1064
```

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:

```
keytool -exportcert -v -alias webcenter -keystore webcenter.jks -storepass  
keystore_password -rfc -file webcenter_public.cer
```

Where:

- *keystore_password* is the keystore password, (for example, `welcome1`)

Example 34–13 Exporting the Certificate Containing the Public Key

```
keytool -exportcert -v -alias webcenter -keystore webcenter.jks -storepass  
welcome1 -rfc -file webcenter_public.cer
```

4. Import the orakey certificate:

```
keytool -importcert -alias orakey -file orakey.cer -keystore webcenter.jks  
-storepass keystore_password
```

Where:

- *keystore_password* is the keystore password, (for example, `welcome1`)

Example 34–14 Importing the orakey Certificate

```
keytool -importcert -alias orakey -file orakey.cer -keystore webcenter.jks  
-storepass welcome1
```

5. Continue by configuring the keystore using either WLST, as described in [Section 34.3.2.2, "Configuring the Keystore Using WLST,"](#) or using Fusion Middleware Control, as described in [Section 34.3.2.3, "Configuring the Keystore Using Fusion Middleware Control."](#)

[Table 34–6](#) shows the keystore contents you should wind up with after creating and configuring the keystore.

Table 34–6 WebCenter Portal Domain Keystore Contents for a Complex Topology

Key Alias	Description
webcenter	Key pair used to sign and encrypt outbound messages from Spaces. This key is used by both OWSM (Portlets and Worklist) and Discussions.
orakey	Certificate containing the public key for the BPEL private key used in the SOA 1 domain. The certificate is used to encrypt outbound messages from the Worklist service to SOA_Server3 in the SOA 1 domain.
soa_server3_public_key	Certificate containing the public key for the soa_server3 private key used in the SOA 2 domain. The certificate is used to encrypt outbound messages from the Worklist service to BPEL Server2 in SOA 2 domain.
producer_public_key	Certificate containing public key for the producer private key used in the external portlet domain that hosts the WSRP Producer 1 application. This certificate is used to encrypt outbound messages from Spaces to WSRP Producer 1 registered in the Spaces application.
external_webcenter_custom_public_key	Certificate containing the public key for the external_webcenter_custom private key used in the external WebCenter Portal domain that hosts the WebCenter Portal application that makes WebService call to the Spaces WebService. This certificate is used to encrypt outbound messages from Spaces to WebCenter Portal applications in the external WebCenter Portal domain.
owc_discussions_public	Certificate containing public key for the external owc_discussions private key used in the external Discussions domain that hosts the Discussions application. This certificate is used by Spaces and WebCenter Portal applications make WebService calls to the Discussions WebService.

34.3.2.2 Configuring the Keystore Using WLST

After creating the WebCenter Portal domain keystore, configure the keystore service and update the credential store so that OWSM can read the keystore and keys correctly.

To configure the keystore service:

1. Go to the `<DOMAIN_HOME>/config/fmwconfig` directory, and open the file `jps-config.xml` in an editor.
2. Locate the `<serviceInstance` node for the `keystore.provider` Provider
3. Ensure that the `webcenter.jks` keystore file is copied to the `<DOMAIN_HOME>/config/fmwconfig` directory, and then specify the location as `./webcenter.jks`.
4. Use the following WLST commands to update the credential store:

```
updateCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password="welcome1", desc="Keystore key")
updateCred(map="oracle.wsm.security", key="enc-csf-key", user="webcenter",
password="welcome1", desc="Encryption key")
updateCred(map="oracle.wsm.security", key="sign-csf-key", user="webcenter",
password="welcome1", desc="Signing key")
```

5. Restart all servers.

34.3.2.3 Configuring the Keystore Using Fusion Middleware Control

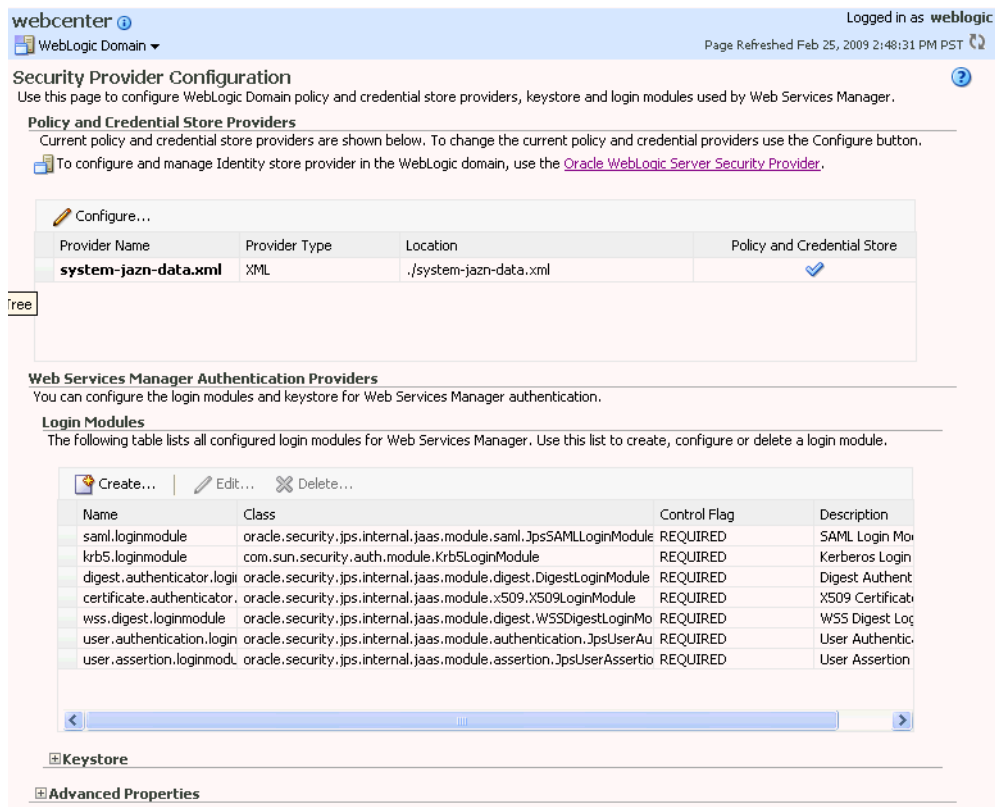
After creating the keystore, configure the keystore service and update the credential store so that OWSM can read the keystore and keys correctly.

To configure the keystore provider:

1. Open Fusion Middleware Control and log in to the WebCenter Portal domain.
For information on logging in to Fusion Middleware Control, see [Chapter 6, "Starting Enterprise Manager Fusion Middleware Control."](#)
2. In the Navigation pane, expand the WebLogic Domain node and click the WebCenter Portal domain (wc_domain by default).
3. From the WebLogic Domain menu, select **Security -> Security Provider Configuration**.

The Security Provider Configuration page displays (see [Figure 34–18](#)).

Figure 34–18 Security Provider Configuration Page



4. Expand the Keystore section on the Security Provider Configuration page.
5. Click **Configure**.

The Keystore Configuration page displays (see [Figure 34–19](#)).

Figure 34–19 Keystore Configuration Page

Security Provider Configuration > Configure Key Store

Information
All changes made in this page require a server restart to take effect.

Keystore Configuration OK Cancel

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 will need to provide the keystore name, path, password and information about default identity certificates.

Keystore Type

Access Attributes

* 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.

<p>Signature Key</p> <p>* Key Alias <input type="text" value="webcenter"/></p> <p>* Signature Password <input type="password" value="....."/></p> <p>* Confirm Password <input type="password" value="....."/></p>	<p>Encryption Key</p> <p>* Crypt Alias <input type="text" value="webcenter"/></p> <p>* Crypt Password <input type="password" value="....."/></p> <p>* Confirm Password <input type="password" value="....."/></p>
---	--

6. Use the following settings to specify the location of the keystore that contains the certificate and private key, and the signature key and encryption key aliases:
 - **Keystore Path:** `./webcenter.jks`
 - **Password:** Enter and confirm the password for the keystore.
 - **Key Alias:** `webcenter`
 - **Signature Password:** Enter and confirm the password for the signature key.
 - **Crypt Alias:** `webcenter`
 - **Crypt Password:** Enter and confirm the password for the encryption key.
7. Click **OK** to save your settings.
8. Restart the Administration server for the domain.

34.3.3 Configuring the Discussions Server for a Complex Topology

In a complex topology, the discussions server is in a different domain than Spaces and consequently you will need to create and configure a keystore for the discussions server and export the certificate containing the public key and import it into the WebCenter Portal domain. For production environments you will also need to protect the Discussion service Web Service end points with an OWSM policy and configure the discussions server connection settings. These configuration steps are described in the following subsections:

- [Section 34.3.3.1, "Securing the Discussions Service End Points"](#)
- [Section 34.3.3.2, "Creating the Discussions Server Keystore"](#)
- [Section 34.3.3.3, "Updating the Credential Store"](#)
- [Section 34.3.3.4, "Configuring the Discussions Server Connection Settings"](#)

Note: Discussions-specific Web Services messages sent by Framework applications to the WebCenter Portal's Discussions Server are not encrypted. For message confidentiality, the discussions server URL must be accessed over Secure Socket Layer (SSL). For more information, see [Chapter 33, "Configuring SSL."](#)

34.3.3.1 Securing the Discussions Service End Points

The WebCenter Portal's Discussions service Web Service end points require user identity to be propagated for calls originating from Spaces. Follow the steps in [Section 34.1.3.1, "Securing the Discussions Service End Points"](#) to secure the endpoints using either Fusion Middleware Control or WLST.

34.3.3.2 Creating the Discussions Server Keystore

This section describes how to create a keystore for the discussions server that contains the key pair used by OWSM, and export the certificate containing the public key so it can be imported into the WebCenter Portal domain.

To create the `owc_discussions` keystore:

1. Go to `JDK_HOME/jdk/bin` and open a command prompt.
2. Using `keytool`, generate a key pair for the `owc_discussions` keystore:

```
keytool -genkeypair -keyalg RSA -dname "consumer_dname" -alias owc_discussions  
-keypass key_password -keystore keystore -storepass keystore_password -validity  
days_valid
```

Where:

- `consumer_dname` is the name of the consumer (for example, `cn=owc_discussions,dc=example,dc=com`)
- `key_password` is the password for the new public key, (for example, `welcome1`)
- `keystore` is the keystore name, (for example, `owc_discussions.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, `1064`).

Example 34–15 Generating the Keypair

```
keytool -genkeypair -keyalg RSA -dname "cn=owc_discussions,dc=example,dc=com"  
-alias owc_discussions -keypass welcome1 -keystore owc_discussions.jks -storepass  
welcome1 -validity 1064
```

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:

```
keytool -exportcert -v -alias owc_discussions -keystore owc_discussions.jks  
-storepass keystore_password -rfc -file owc_discussions_public.cer
```

Where:

- `keystore_password` is the keystore password, (for example, `welcome1`)

Example 34–16 Exporting the Certificate Containing the Public Key

```
keytool -exportcert -v -alias owc_discussions -keystore owc_discussions.jks
-storepass welcome1 -rfc -file owc_discussions_public.cer
```

4. Import the webcenter_public certificate:

```
keytool -importcert -alias webcenter_public -file webcenter_public.cer
-keystore owc_discussions.jks -storepass keystore_password
```

Where:

- `keystore_password` is the keystore password, (for example, `welcome1`)

Example 34–17 Importing the webcenter_public Certificate

```
keytool -importcert -alias webcenter_public -file webcenter_public.cer -keystore
owc_discussions.jks -storepass welcome1
```

5. Import the owc_discussions_public certificate:

```
keytool -importcert -alias owc_discussions_public -file
owc_discussions_public.cer -keystore webcenter.jks -storepass keystore_password
```

Where:

- `keystore_password` is the keystore password, (for example, `welcome1`)

Example 34–18 Importing the owc_discussions_public Certificate

```
keytool -importcert -alias owc_discussions_public -file owc_discussions_public.cer
-keystore webcenter.jks -storepass welcome1
```

6. Continue by updating the credential store using WLST as described in [Section 34.3.3.3, "Updating the Credential Store."](#)

34.3.3.3 Updating the Credential Store

After creating the WebCenter Portal domain keystore, configure the keystore service and update the credential store so that OWSM can read the keystore and keys correctly.

To configure the keystore service:

1. Go to the `<DOMAIN_HOME>/config/fmwconfig` directory, and open the file `jps-config.xml` in an editor.
2. Locate the `<serviceInstance` node for the `keystore.provider` Provider:

```
<!-- KeyStore Service Instance -->
<serviceInstance name="keystore" provider="keystore.provider"
location="./default-keystore.jks">
<description>Default JPS Keystore Service</description>
```

3. Make sure that the `webcenter.jks` keystore file is copied to the `<DOMAIN_HOME>/config/fmwconfig` directory, and then specify the location as `./webcenter.jks`.

```
<serviceInstance name="keystore" provider="keystore.provider"
location="./webcenter.jks">
```

```
<description>Default JPS Keystore Service</description>
```

4. Use the following WLST commands to update the credential store:

```
updateCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password="welcome1", desc="Keystore key")
updateCred(map="oracle.wsm.security", key="enc-csf-key",
user="owc_discussions", password="welcome1", desc="Encryption key")
updateCred(map="oracle.wsm.security", key="sign-csf-key",
user="owc_discussions", password="welcome1", desc="Signing key")
```

5. Restart all servers.

34.3.3.4 Configuring the Discussions Server Connection Settings

You must supply the WS-Security client certificate information within the discussions server connection that is configured for Spaces or your Framework application, as described in [Section 14.3, "Registering Discussions Servers."](#) [Figure 34–20](#) shows example connection detail settings for the Edit Discussions and Announcement Connection page.

Figure 34–20 Edit Discussions and Announcement Connection Page

Edit Discussion and Announcement Connection ?

Name

Connection Name

Active Connection

Connection Details

* Server URL

* Administrator User Name

Authenticated User WebService Policy URI

Public User WebService Policy URI

* Recipient Key Alias

Advanced Configuration

Specify additional (optional) configuration properties for the connection.

Connection Timeout (seconds)

Additional Properties

Enter names and values for any additional properties.

Property Name	Property Value	Is Property Secured?
No Data Available		

34.3.4 Setting Up the First SOA Domain

This section describes how to set up the SOA domain keystore and contains the following subsections:

- [Section 34.3.4.1, "Creating the SOA Domain Keystore"](#)
- [Section 34.3.4.2, "Configuring the Keystore Using WLST"](#)
- [Section 34.3.4.3, "Configuring the Keystore Using Fusion Middleware Control"](#)

34.3.4.1 Creating the SOA Domain Keystore

This section describes how to create a SOA domain keystore and keys using a Java Keystore (JKS).

To create the SOA domain keystore:

1. Go to `JDK_HOME/jdk/bin` and open a command prompt.
2. Create a keystore by importing the public certificate (`webcenter_public.cer`) from the WebCenter Portal domain:

```
keytool -importcert -alias webcenter_spaces_ws -file webcenter_public.cer
-keystore bpel.jks -storepass keystore_password
```

Where:

- `keystore_password` is the keystore password, (for example, `welcome1`)

Example 34–19 Importing the Public Certificate

```
keytool -importcert -alias webcenter_spaces_ws -file webcenter_public.cer
-keystore bpel.jks -storepass welcome1
```

3. Using `keytool`, create a keypair to be used in the SOA domain for signing and encrypting messages:

```
keytool -genkeypair -keyalg RSA -dname "consumer_dname" -alias bpel -keypass
key_password -keystore bpel.jks -storepass keystore_password -validity
days_valid
```

Where:

- `consumer_dname` is the name of the consumer (for example, `cn=bpel,dc=example,dc=com`)
- `key_password` is the password for the new public key, (for example, `welcome1`)
- `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, `1064`).

Example 34–20 Generating the Keypair

```
keytool -genkeypair -keyalg RSA -dname "cn=bpel,dc=example,dc=com" -alias bpel
-keypass welcome1 -keystore bpel.jks -storepass welcome1 -validity 1064
```

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.

4. Export the certificate so it can be imported in the WebCenter Portal domain using the `orakey` alias:

```
keytool -exportcert -v -alias bpel -keystore bpel.jks -storepass
keystore_password -rfc -file orakey.cer
```

Where:

- `keystore_password` is the keystore password (for example, `welcome1`)

Example 34–21 Exporting the Certificate Containing the Public Key

```
keytool -exportcert -v -alias bpel -keystore bpel.jks -storepass welcome1 -rfc
-file orakay.cer
```

5. Import the certificate to the WebCenter Portal domain again with a different alias (choose **Yes** when prompted whether to overwrite the existing certificate with the alias orakey):

```
keytool -importcert -alias orakey -file orakey.cer -keystore webcenter.jks
-storepass keystore_password
```

Where:

- `keystore_password` is the keystore password (for example, `welcome1`)

Example 34–22 Importing the Certificate

```
keytool -importcert -alias orakey -file orakay.cer -keystore webcenter.jks
-storepass welcome1
```

6. Import the certificate to the into the SOA domain:

```
keytool -importcert -alias soa_server3_public_key -file
soa_server3_public_key.cer -keystore webcenter.jks -storepass keystore_password
```

Where:

- `keystore_password` is the keystore password (for example, `welcome1`)

Example 34–23 Importing the Certificate

```
keytool -importcert -alias soa_server3_public_key -file soa_server3_public_key.cer
-keystore webcenter.jks -storepass welcome1
```

7. Continue by configuring the keystore using either WLST, as described in [Section 34.3.4.2, "Configuring the Keystore Using WLST,"](#) or using Fusion Middleware Control as described in [Section 34.3.4.3, "Configuring the Keystore Using Fusion Middleware Control."](#)

[Table 34–7](#) shows the keystore contents you should wind up with after creating and configuring the SOA 1 domain keystore.

Table 34–7 SOA 1 Domain Keystore Contents for a Complex Topology

Key Alias	Description
bpel	Private key used to sign outbound messages from the SOA 1 domain servers. This key is used by the Worklist application deployed on the SOA 1 domain's SOA server.
webcenter_spaces_ws	Certificate containing the public key for the webcenter private key used in the WebCenter Portal domain. The certificate is used to encrypt outbound Workflow messages on BPEL Server1 in the SOA 1 domain to WebService APIs on the Spaces domain.

34.3.4.2 Configuring the Keystore Using WLST

After creating the SOA domain keystore, configure the keystore service and update the credential store so that OWSM can read the keystore and keys correctly. You can do this using either Fusion Middleware Control, as described in [Section 34.3.4.3, "Configuring the Keystore Using Fusion Middleware Control,"](#) or using WLST as described below.

To configure the keystore service:

1. Go to the `<DOMAIN_HOME>/config/fmwconfig` directory, and open the file `jps-config.xml` in an editor.

2. Locate the <serviceInstance node for the keystore.provider Provider
3. Ensure that the bpel.jks keystore file is copied to the <DOMAIN_HOME>/config/fmwconfig directory, and then specify the location as ./bpel.jks.
4. Use the following WLST commands to update the credential store:


```
updateCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password="welcome1", desc="Keystore key")
updateCred(map="oracle.wsm.security", key="enc-csf-key", user="bpel",
password="welcome1", desc="Encryption key")
updateCred(map="oracle.wsm.security", key="sign-csf-key", user="bpel",
password="welcome1", desc="Signing key")
```
5. Restart all servers.

34.3.4.3 Configuring the Keystore Using Fusion Middleware Control

After creating the keystore, configure the keystore service and update the credential store so that OWSM can read the keystore and keys correctly. You can do this using either WLST, as described in [Section 34.3.4.2, "Configuring the Keystore Using WLST,"](#) or using Fusion Middleware Control as described below.

To configure the keystore provider:

1. Open Fusion Middleware Control and log in to the WebCenter Portal domain.
For information on logging in to Fusion Middleware Control, see [Chapter 6, "Starting Enterprise Manager Fusion Middleware Control."](#)
2. In the Navigation pane, expand the WebLogic Domain node and click the SOA domain.
3. From the SOA Domain menu, select **Security -> Security Provider Configuration**.
4. Expand the Keystore section on the Security Provider Configuration page.
5. Click **Configure**.

The Keystore Configuration page displays (see [Figure 34-21](#)).

Figure 34-21 Keystore Configuration Page

Security Provider Configuration > Configure Key Store

Information
All changes made in this page require a server restart to take effect.

Keystore Configuration OK Cancel

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 will need to provide the keystore name, path, password and information about default identity certificates.

Keystore Type:

Access Attributes

* 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.

<p>Signature Key</p> <p>* Key Alias: <input type="text" value="bpel"/></p> <p>* Signature Password: <input type="password" value="....."/></p> <p>* Confirm Password: <input type="password" value="....."/></p>	<p>Encryption Key</p> <p>* Crypt Alias: <input type="text" value="bpel"/></p> <p>* Crypt Password: <input type="password" value="....."/></p> <p>* Confirm Password: <input type="password" value="....."/></p>
---	--

6. Use the following settings to specify the location of the keystore that contains the certificate and private key, and the signature key and encryption key aliases:
 - **Keystore Path:** `./bpe1.jks`
 - **Password:** Enter and confirm the password for the keystore.
 - **Key Alias:** `bpe1`
 - **Signature Password:** Enter and confirm the password for the signature key.
 - **Crypt Alias:** `bpe1`
 - **Crypt Password:** Enter and confirm the password for the encryption key.
7. Click **OK** to save your settings.
8. Restart the Administration server for the domain.

34.3.5 Setting Up the Second SOA Domain

This section describes how to set up a second SOA domain keystore and contains the following subsections:

- [Section 34.3.5.1, "Creating the SOA Domain Keystore"](#)
- [Section 34.3.5.2, "Configuring the Keystore Using WLST"](#)
- [Section 34.3.5.3, "Configuring the Keystore Using Fusion Middleware Control"](#)
- [Section 34.3.5.4, "Configuring the Spaces Worklist Connection for the Second SOA Server"](#)

34.3.5.1 Creating the SOA Domain Keystore

This section describes how to create a SOA domain keystore and keys using a Java Keystore (JKS).

To create the SOA domain keystore:

1. Go to `JDK_HOME/jdk/bin` and open a command prompt.
2. Using `keytool`, create a keypair to be used in the SOA domain for signing and encrypting messages:

```
keytool -genkeypair -keyalg RSA -dname "consumer_dname" -alias soa_server3
-keypass key_password -keystore soa_server3.jks -storepass keystore_password
-validity days_valid
```

Where:

- `consumer_dname` is the name of the consumer (for example, `cn=soa_server3,dc=example,dc=com`)
- `key_password` is the password for the new public key, (for example, `welcome1`)
- `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, `1064`).

Example 34–24 Generating the Keypair

```
keytool -genkeypair -keyalg RSA -dname "cn=soa_server3,dc=example,dc=com" -alias
soa_server3 -keypass welcome1 -keystore soa_server3.jks -storepass welcome1
-validity 1064
```

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 so it can be imported in the WebCenter Portal domain using the `orakey` alias:

```
keytool -exportcert -v -alias soa_server3 -keystore soa_server3.jks
-storepass keystore_password -rfc -file soa_server3_public_key.cer
```

Where:

- `keystore_password` is the keystore password, (for example, `welcome1`)

Example 34–25 Exporting the Certificate Containing the Public Key

```
keytool -exportcert -v -alias soa_server3 -keystore soa_server3.jks
-storepass welcome1 -rfc -file soa_server3_public_key.cer
```

4. Import the certificate to the WebCenter Portal domain with a different alias (choose **Yes** when prompted whether to overwrite the existing certificate with the alias `soa_server3_public_key`):

```
keytool -importcert -alias soa_server3_public_key -file soa_server3_public_
key.cer -keystore webcenter.jks -storepass keystore_password
```

Where:

- `keystore_password` is the keystore password (for example, `welcome1`)

Example 34–26 Importing the Certificate

```
keytool -importcert -alias soa_server3_public_key -file soa_server3_public_key.cer
-keystore webcenter.jks -storepass welcome1
```

5. Import the `soa_server3_public_key` certificate:

```
keytool -importcert -alias soa_server3_public_key -file
soa_server3_public_key.cer -keystore webcenter.jks -storepass keystore_password
```

Where:

- `keystore_password` is the keystore password, (for example, `welcome1`)

Example 34–27 Importing the soa_server3_public_key Certificate

```
keytool -importcert -alias soa_server3_public_key -file soa_server3_public_key.cer
-keystore webcenter.jks -storepass welcome1
```

6. Import the `producer_public_key` certificate:

```
keytool -importcert -alias producer_public_key -file producer_public_key.cer
-keystore webcenter.jks -storepass keystore_password
```

Where:

- `keystore_password` is the keystore password, (for example, `welcome1`)

Example 34–28 Importing the producer_public_key Certificate

```
keytool -importcert -alias producer_public_key -file producer_public_key.cer
-keystore webcenter.jks -storepass welcome1
```

7. Import the external_webcenter_custom_public_key certificate:

```
keytool -importcert -alias external_webcenter_custom_public_key -file
external_webcenter_custom_public_key.cer -keystore webcenter.jks -storepass
keystore_password
```

Where:

- *keystore_password* is the keystore password, (for example, welcome1)

Example 34–29 Importing the external_webcenter_custom_public_key Certificate

```
keytool -importcert -alias external_webcenter_custom_public_key -file
external_webcenter_custom_public_key.cer -keystore webcenter.jks -storepass
welcome1
```

8. Continue by configuring the keystore using either WLST, as described in Section 34.3.5.2, "Configuring the Keystore Using WLST," or using Fusion Middleware Control as described in Section 34.3.5.3, "Configuring the Keystore Using Fusion Middleware Control."

Table 34–8 shows the keystore contents you should wind up with after creating and configuring the SOA 2 domain keystore.

Table 34–8 SOA 2 Domain Keystore Contents for a Complex Topology

Key Alias	Description
webcenter	Key pair used to sign and encrypt outbound messages from Spaces. This key is used by both OWSM (Portlets and Worklist) and Discussions.
orakey	Certificate containing the public key for the BPEL private key used in the SOA 1 domain. The certificate is used to encrypt outbound messages from the Worklist service to SOA_Server3 in the SOA 1 domain.
soa_server3_public_key	Certificate containing the public key for the soa_server3 private key used in the SOA 2 domain. The certificate is used to encrypt outbound messages from the Worklist service to BPEL Server2 in SOA 2 domain.
producer_public_key	Certificate containing public key for the producer private key used in the external portlet domain that hosts the WSRP Producer 1 application. This certificate is used to encrypt outbound messages from Spaces to WSRP Producer 1 registered in the Spaces application.
external_webcenter_custom_public_key	Certificate containing the public key for the external_webcenter_custom private key used in the external WebCenter Portal domain that hosts the Framework application that makes WebService call to the Spaces WebService. This certificate is used to encrypt outbound messages from Spaces to Framework applications in the external WebCenter Portal domain.

34.3.5.2 Configuring the Keystore Using WLST

After creating the second SOA domain keystore, configure the keystore service and update the credential store so that OWSM can read the keystore and keys correctly. You can do this using either Fusion Middleware Control, as described in

[Section 34.3.5.3, "Configuring the Keystore Using Fusion Middleware Control,"](#) or using WLST as described below.

To configure the keystore service:

1. Go to the `<DOMAIN_HOME>/config/fmwconfig` directory, and open the file `jps-config.xml` in an editor.
2. Locate the `<serviceInstance` node for the keystore.provider Provider
3. Ensure that the `soa_server3.jks` keystore file is copied to the `<DOMAIN_HOME>/config/fmwconfig` directory, and then specify the location as `./soa_server3.jks`.

4. Use the following WLST commands to update the credential store:

```
updateCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password="welcome1", desc="Keystore key")
updateCred(map="oracle.wsm.security", key="enc-csf-key", user="soa_server3",
password="welcome1", desc="Encryption key")
updateCred(map="oracle.wsm.security", key="sign-csf-key", user="soa_server3",
password="welcome1", desc="Signing key")
```

5. Restart all servers.

34.3.5.3 Configuring the Keystore Using Fusion Middleware Control

After creating the keystore, configure the keystore service and update the credential store so that OWSM can read the keystore and keys correctly. You can do this using either WLST, as described in [Section 34.3.5.2, "Configuring the Keystore Using WLST,"](#) or using Fusion Middleware Control as described below.

To configure the keystore provider:

1. Open Fusion Middleware Control and log in to the WebCenter Portal domain.
For information on logging in to Fusion Middleware Control, see [Chapter 6, "Starting Enterprise Manager Fusion Middleware Control."](#)
2. In the Navigation pane, expand the WebLogic Domain node and click the SOA domain.
3. From the SOA Domain menu, select **Security -> Security Provider Configuration**.
4. Expand the Keystore section on the Security Provider Configuration page.
5. Click **Configure**.

The Keystore Configuration page displays (see [Figure 34-22](#)).

Figure 34–22 Keystore Configuration Page

Security Provider Configuration > Configure Key Store

Information
All changes made in this page require a server restart to take effect.

Keystore Configuration OK Cancel

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 will need to provide the keystore name, path, password and information about default identity certificates.

Keystore Type:

Access Attributes

* 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" value="soa_server3"/>	* Crypt Alias: <input type="text" value="soa_server3"/>
* Signature Password: <input type="password" value="....."/>	* Crypt Password: <input type="password" value="....."/>
* Confirm Password: <input type="password" value="....."/>	* Confirm Password: <input type="password" value="....."/>

6. Use the following settings to specify the location of the keystore that contains the certificate and private key, and the signature key and encryption key aliases:
 - **Keystore Path:** `./soa_server3.jks`
 - **Password:** Enter and confirm the password for the keystore.
 - **Key Alias:** `soa_server3`
 - **Signature Password:** Enter and confirm the password for the signature key.
 - **Crypt Alias:** `soa_server3`
 - **Crypt Password:** Enter and confirm the password for the encryption key.
7. Click **OK** to save your settings.
8. Restart the Administration server for the domain.

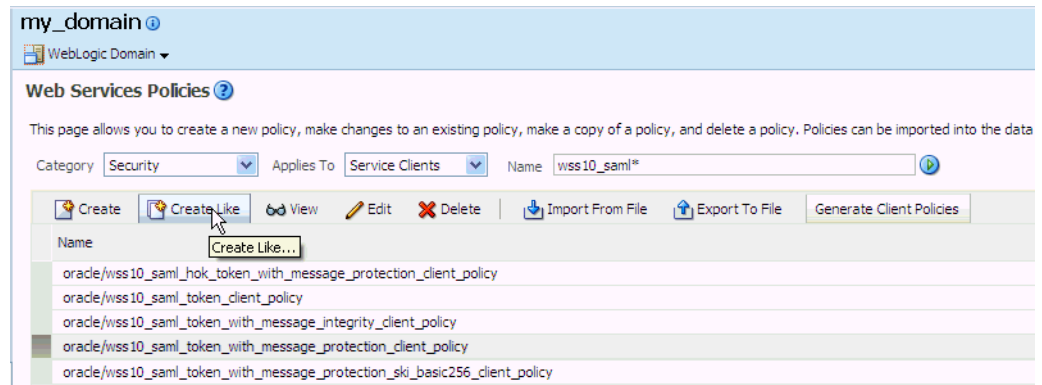
34.3.5.4 Configuring the Spaces Worklist Connection for the Second SOA Server

Ordinarily, the Spaces Worklist connections uses the `oracle/wss10_saml_token_with_message_protection_client_policy` policy to secure outbound SOAP messages to SOA Server. However, in a complex deployment where the WebCenter Portal domain uses two or more Worklist connections simultaneously we need to create an additional OWSM policy and configure it so that the recipient key alias matches the alias of the certificate of the intended SOA server on the Spaces side.

Follow the steps below to use multiple Worklist connections simultaneously:

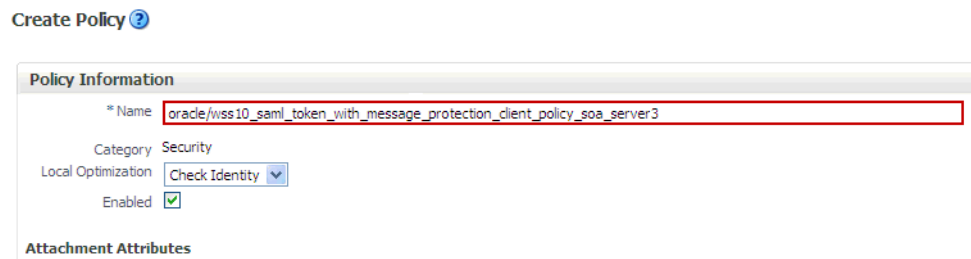
1. Export the certificate from the external SOA domain and import it into the WebCenter Portal domain under a new alias (`soa_server3_key` in the following example).
2. Use Fusion Middleware Control to create a new OWSM policy, and override the recipient key alias to use the same alias as above.
 - a. In Fusion Middleware Control, from the WebLogic domain menu select **Web Services -> Policies**.

The Web Services Policies page displays (see [Figure 34–23](#)).

Figure 34–23 Web Services Policies Page

- b. Select a client policy to use as a base for creating the new policy and click **Create Like**.

The Create Policy page displays (see [Figure 34–24](#)).

Figure 34–24 Create Policy Page

- c. Enter a name for the new policy (for example, `oracle_wss10_saml_token_with_message_protection_client_policy_soa_server3`) and click **Save**.

The new policy should now be listed on the Web Services Policies page.

- d. From the Web Services Policy page, select the new policy and click **Edit**.
 - e. On the Edit Policy page, open the Configuration tab and click **Edit**.
 - f. Override the recipient key alias with the value `soa_server3_key` and click **Save**.
3. Create the BPEL connection to set the security policy to the policy created above using the following WLST command:

```
setBPELConnection (appName='webcenter' ,
name='WebCenter-Worklist-SOAServer3' ,url='<your_url>' ,
policy='oracle/wss10_saml_token_with_message_protection_client_policy_soa_server3')
```

34.3.6 Setting Up the External Portlet Domain Keystore

This section describes how to set up the keystore for the external portlet domain used by one of the WSRP producers for this complex topology.

This section contains the following subsections:

- [Section 34.3.6.1, "Creating the External Portlet Domain Keystore"](#)

- [Section 34.3.6.2, "Configuring the Keystore Using WLST"](#)
- [Section 34.3.6.3, "Configuring the Keystore Using Fusion Middleware Control"](#)

34.3.6.1 Creating the External Portlet Domain Keystore

To create the external portlet domain keystore:

1. Go to `JDK_HOME/jdk/bin` and open a command prompt.
2. Using `keytool`, generate the keystore by importing the WebCenter Portal domain's public certificate:

```
keytool -importcert -alias webcenter_public -file webcenter_public.cer
-keystore producer.jks -storepass keystore_password
```

Where:

- `keystore_password` is the keystore password

Example 34–30 Importing the Certificate

```
keytool -importcert -alias webcenter_public -file webcenter_public.cer -keystore
producer.jks -storepass welcome1
```

3. Using `keytool`, generate a key pair:

```
keytool -genkeypair -keyalg RSA -dname "consumer_dname" -alias producer
-keypass key_password -keystore producer.jks -storepass keystore_password
-validity days_valid
```

Where:

- `consumer_dname` is the name of the consumer (for example, `cn=producer,dc=example,dc=com`)
- `key_password` is the password for the new public key, (for example, `welcome1`)
- `keystore` is the keystore name, (for example, `webcenter.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, `1064`).

Example 34–31 Generating the Keypair

```
keytool -genkeypair -keyalg RSA -dname "cn=producer,dc=example,dc=com" -alias
producer -keypass welcome1 -keystore producer.jks -storepass welcome1 -validity
1064
```

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.

4. Export the certificate containing the public key so that it can be imported into the Spaces domain's keystore:

```
keytool -exportcert -v -alias producer -keystore producer.jks -storepass
keystore_password -rfc -file producer_public_key.cer
```

Where:

- `keystore_password` is the keystore password, (for example, `welcome1`)

Example 34–32 Exporting the Certificate Containing the Public Key

```
keytool -exportcert -v -alias producer -keystore producer.jks -storepass welcome1
-rfc -file producer_public_key.cer
```

5. Import the certificate to the WebCenter Portal domain with a different alias (choose **Yes** when prompted whether to overwrite the existing certificate with the alias `producer_public_key`):

```
keytool -importcert -alias producer_public_key -file producer_public_key.cer
-keystore webcenter.jks -storepass keystore_password
```

Where:

- `keystore_password` is the keystore password (for example, `welcome1`)

Example 34–33 Importing the Certificate

```
keytool -importcert -alias producer_public_key -file producer_public_key.cer
-keystore webcenter.jks -storepass welcome1
```

6. Continue by configuring the keystore using either WLST as described in [Section 34.3.6.2, "Configuring the Keystore Using WLST,"](#) or using Fusion Middleware Control as described in [Section 34.3.6.3, "Configuring the Keystore Using Fusion Middleware Control."](#)

34.3.6.2 Configuring the Keystore Using WLST

After creating the external portlet domain keystore, configure the keystore service and update the credential store so that OWSM can read the keystore and keys correctly. You can do this using either Fusion Middleware Control, as described in [Section 34.3.6.3, "Configuring the Keystore Using Fusion Middleware Control,"](#) or using WLST as described below.

To configure the keystore service:

1. Go to the `<DOMAIN_HOME>/config/fmwconfig` directory, and open the file `jps-config.xml` in an editor.
2. Locate the `<serviceInstance` node for the keystore.provider Provider
3. Ensure that the `producer.jks` keystore file is copied to the `<DOMAIN_HOME>/config/fmwconfig` directory, and then specify the location as `./producer.jks`.

4. Use the following WLST commands to update the credential store:

```
updateCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password="welcome1", desc="Keystore key")
updateCred(map="oracle.wsm.security", key="enc-csf-key", user="producer",
password="welcome1", desc="Encryption key")
updateCred(map="oracle.wsm.security", key="sign-csf-key", user="producer",
password="welcome1", desc="Signing key")
```

5. Restart all servers.

34.3.6.3 Configuring the Keystore Using Fusion Middleware Control

After creating the keystore, configure the keystore service and update the credential store so that OWSM can read the keystore and keys correctly. You can do this using either WLST, as described in [Section 34.3.6.2, "Configuring the Keystore Using WLST,"](#) or using Fusion Middleware Control as described below.

To configure the keystore provider:

1. Open Fusion Middleware Control and log in to the WebCenter Portal domain.
For information on logging in to Fusion Middleware Control, see [Chapter 6, "Starting Enterprise Manager Fusion Middleware Control."](#)
2. In the Navigation pane, expand the WebLogic Domain node and click the WebCenter Portal domain (wc_domain by default).
3. From the WebLogic Domain menu, select **Security -> Security Provider Configuration**.
4. Expand the Keystore section on the Security Provider Configuration page.
5. Click **Configure**.

The Keystore Configuration page displays (see [Figure 34–25](#)).

Figure 34–25 Keystore Configuration Page

Security Provider Configuration > Configure Key Store

Information
All changes made in this page require a server restart to take effect.

Keystore Configuration OK Cancel

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 will need to provide the keystore name, path, password and information about default identity certificates.

Keystore Type:

Access Attributes

* 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.

<p>Signature Key</p> <p>* Key Alias: <input type="text" value="producer"/></p> <p>* Signature Password: <input type="password" value="....."/></p> <p>* Confirm Password: <input type="password" value="....."/></p>	<p>Encryption Key</p> <p>* Crypt Alias: <input type="text" value="producer"/></p> <p>* Crypt Password: <input type="password" value="....."/></p> <p>* Confirm Password: <input type="password" value="....."/></p>
---	--

6. Use the following settings to specify the location of the keystore that contains the certificate and private key, and the signature key and encryption key aliases:
 - **Keystore Path:** ./producer.jks
 - **Password:** Enter and confirm the password for the keystore.
 - **Key Alias:** producer
 - **Signature Password:** Enter and confirm the password for the signature key.
 - **Crypt Alias:** producer
 - **Crypt Password:** Enter and confirm the password for the encryption key.
7. Click **OK** to save your settings.
8. Restart the Administration server for the domain.

34.3.7 Setting Up the External WebCenter Portal Domain Keystore

This section describes how to set up an external WebCenter Portal domain used by a Framework application making Spaces WebService calls.

This section contains the following subsections:

- [Section 34.3.7.1, "Creating the External WebCenter Portal Domain Keystore"](#)
- [Section 34.3.7.2, "Configuring the Keystore Using WLST"](#)
- [Section 34.3.7.3, "Configuring the Keystore Using Fusion Middleware Control"](#)

34.3.7.1 Creating the External WebCenter Portal Domain Keystore

To create the external WebCenter Portal domain keystore:

1. Go to `JDK_HOME/jdk/bin` and open a command prompt.
2. Using `keytool`, generate the keystore by importing the WebCenter Portal domain's public certificate:

```
keytool -importcert -alias webcenter_public -file webcenter_public.cer
-keystore external_webcenter_custom.jks -storepass keystore_password
```

Where:

- `keystore_password` is the keystore password

Example 34–34 Importing the Certificate

```
keytool -importcert -alias webcenter_public -file webcenter_public.cer -keystore
external_webcenter_custom.jks -storepass welcome1
```

3. Using `keytool`, generate a key pair:

```
keytool -genkeypair -keyalg RSA -dname "consumer_dname" -alias
external_webcenter_custom -keypass key_password -keystore
external_webcenter_custom.jks
-storepass keystore_password -validity days_valid
```

Where:

- `consumer_dname` is the name of the consumer (for example, `cn=external_webcenter_custom,dc=example,dc=com`)
- `key_password` is the password for the new public key, (for example, `welcome1`)
- `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, `1064`).

Example 34–35 Generating the Keypair

```
keytool -genkeypair -keyalg RSA -dname "cn=external_webcenter_custom,
dc=example,dc=com" -alias external_webcenter_custom -keypass welcome1
-keystore external_webcenter_custom.jks -storepass welcome1 -validity 1064
```

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.

- Export the certificate containing the public key so that it can be imported into the Spaces domain's keystore:

```
keytool -exportcert -v -alias external_webcenter_custom -keystore external_
webcenter_custom.jks -storepass keystore_password -rfc -file external_
webcenter_custom_public_key.cer
```

Where:

- `keystore_password` is the keystore password, (for example, `welcome1`)

Example 34–36 Exporting the Certificate Containing the Public Key

```
keytool -exportcert -v -alias external_webcenter_custom -keystore external_
webcenter_custom.jks -storepass welcome1 -rfc -file external_webcenter_custom_
public_key.cer
```

- Import the certificate to the WebCenter Portal domain with a different alias (choose **Yes** when prompted whether to overwrite the existing certificate with the alias `external_webcenter_custom_public_key`):

```
keytool -importcert -alias external_webcenter_custom_public_key -file external_
webcenter_custom_public_key.cer -keystore webcenter.jks -storepass
keystore_password
```

Where:

- `keystore_password` is the keystore password (for example, `welcome1`)

Example 34–37 Importing the Certificate

```
keytool -importcert -alias external_webcenter_custom_public_key -file external_
webcenter_custom_public_key.cer -keystore webcenter.jks -storepass welcome1
```

- Continue by configuring the keystore using either WLST as described in [Section 34.3.7.2, "Configuring the Keystore Using WLST,"](#) or using Fusion Middleware Control as described in [Section 34.3.7.3, "Configuring the Keystore Using Fusion Middleware Control."](#)

34.3.7.2 Configuring the Keystore Using WLST

After creating the external WebCenter Portal domain keystore, configure the keystore service and update the credential store so that OWSM can read the keystore and keys correctly. You can do this using either Fusion Middleware Control, as described in [Section 34.3.7.3, "Configuring the Keystore Using Fusion Middleware Control,"](#) or using WLST as described below.

To configure the keystore service:

- Go to the `<DOMAIN_HOME>/config/fmwconfig` directory, and open the file `jps-config.xml` in an editor.
- Locate the `<serviceInstance` node for the `keystore.provider Provider`
- Ensure that the `webcenter.jks` keystore file is copied to the `<DOMAIN_HOME>/config/fmwconfig` directory, and then specify the location as `./webcenter.jks`.
- Use the following WLST commands to update the credential store:

```
updateCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password="welcome1", desc="Keystore key")
updateCred(map="oracle.wsm.security", key="enc-csf-key",
```

```
user="external_webcenter_custom", password="welcome1", desc="Encryption key")
updateCred(map="oracle.wsm.security", key="sign-csf-key",
user="external_webcenter_custom", password="welcome1", desc="Signing key")
```

- Restart all servers.

34.3.7.3 Configuring the Keystore Using Fusion Middleware Control

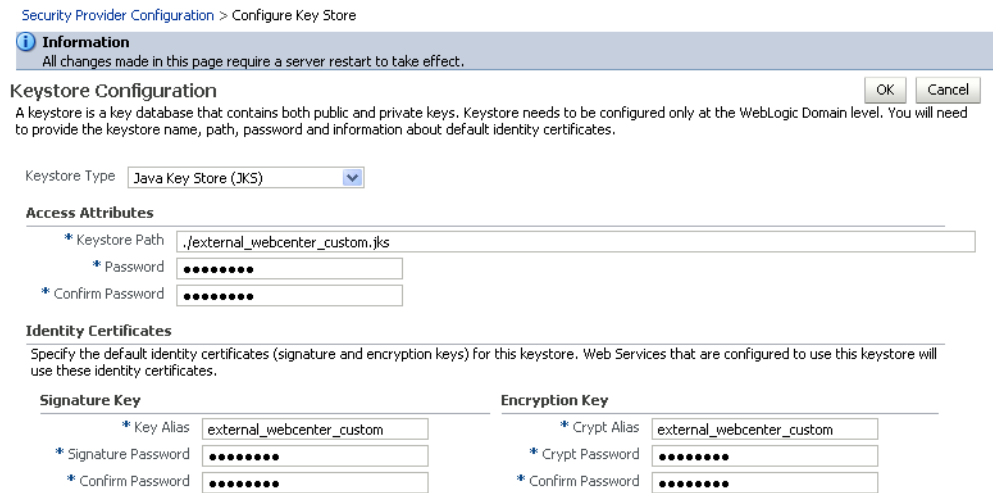
After creating the keystore, configure the keystore service and update the credential store so that OWSM can read the keystore and keys correctly. You can do this using either WLST, as described in [Section 34.3.7.2, "Configuring the Keystore Using WLST,"](#) or using Fusion Middleware Control as described below.

To configure the keystore provider:

- Open Fusion Middleware Control and log in to the WebCenter Portal domain.
For information on logging in to Fusion Middleware Control, see [Chapter 6, "Starting Enterprise Manager Fusion Middleware Control."](#)
- In the Navigation pane, expand the WebLogic Domain node and click the WebCenter Portal domain (wc_domain by default).
- From the WebLogic Domain menu, select **Security -> Security Provider Configuration**.
- Expand the Keystore section on the Security Provider Configuration page.
- Click **Configure**.

The Keystore Configuration page displays (see [Figure 34-26](#)).

Figure 34-26 Keystore Configuration Page



- Use the following settings to specify the location of the keystore that contains the certificate and private key, and the signature key and encryption key aliases:
 - Keystore Path:** ./external_webcenter_custom.jks
 - Password:** Enter and confirm the password for the keystore.
 - Key Alias:** external_webcenter_custom
 - Signature Password:** Enter and confirm the password for the signature key.
 - Crypt Alias:** external_webcenter_custom

- **Crypt Password:** Enter and confirm the password for the encryption key.
- 7. Click **OK** to save your settings.
- 8. Restart the Administration server for the domain.

34.3.8 Command Summary for a Complex Topology

Use the following command summary to quickly configure the keystore and DF properties for a complex topology.

Generate the Keystore

Use the following `keytool` commands to generate the keystore, replacing the values in bold with those for your local environment:

```
keytool -genkeypair -keyalg RSA -dname "cn=spaces,dc=example,dc=com" -alias
webcenter -keypass welcome1 -keystore webcenter.jks -storepass welcome1 -validity
1064
```

```
keytool -exportcert -v -alias webcenter -keystore webcenter.jks -storepass
welcome1 -rfc -file webcenter_public.cer
```

```
keytool -importcert -alias df_webcenter_public -file webcenter_public.cer
-keystore owc_discussions.jks -storepass welcome1
```

When prompted to trust the certificate, say yes.

```
keytool -importcert -alias webcenter_spaces_ws -file webcenter_public.cer
-keystore bpel.jks -storepass welcome1
```

When prompted to trust the certificate, say yes.

```
keytool -genkeypair -keyalg RSA -dname "cn=bpel,dc=example,dc=com" -alias bpel
-keypass welcome1 -keystore bpel.jks
```

```
keytool -exportcert -v -alias bpel -keystore bpel.jks -storepass welcome1 -rfc
-file orakay.cer
```

```
keytool -importcert -alias orakey -file orakay.cer -keystore webcenter.jks
-storepass welcome1
```

When prompted to trust the certificate, say yes.

```
keytool -genkeypair -keyalg RSA -dname "cn=soa_server3,dc=example,dc=com" -alias
soa_server3 -keypass welcome1 -keystore soa_server3.jks -storepass welcome1
-validity 1024
```

```
keytool -exportcert -v -alias soa_server3 -keystore soa_server3.jks -storepass
welcome1 -rfc -file soa_server3_public_key.cer
```

```
keytool -importcert -alias soa_server3_public_key -file soa_server3_public_key.cer
-keystore webcenter.jks -storepass welcome1
```

When prompted to trust the certificate, say yes.

```
keytool -importcert -alias webcenter_public -file webcenter_public.cer -keystore
producer.jks -storepass welcome1
```

When prompted to trust the certificate, say yes.

```
keytool -genkeypair -keyalg RSA -dname "cn=producer,dc=example,dc=com" -alias
producer -keypass welcome1 -keystore producer.jks -storepass welcome1 -validity
1024
```

```
keytool -exportcert -v -alias producer -keystore producer.jks -storepass welcome1
```



```
-rfc -file producer_public_key.cer
```

```
keytool -importcert -alias webcenter_public -file webcenter_public.cer
-keystore external_webcenter_custom.jks -storepass welcome1
```

When prompted to trust the certificate, say yes.

```
keytool -genkeypair -keyalg RSA -dname
"cn=external_webcenter_custom,dc=example,dc=com" -alias external_webcenter_custom
-keypass welcome1 -keystore external_webcenter_custom.jks
-storepass welcome1 -validity 1024
```

```
keytool -exportcert -v -alias external_webcenter_custom -keystore
external_webcenter_custom.jks -storepass welcome1 -rfc -file
external_webcenter_custom_public_key.cer
```

```
keytool -importcert -alias producer_public_key -file producer_public_key.cer
-keystore webcenter.jks -storepass welcome1
```

When prompted to trust the certificate, say yes.

```
keytool -importcert -alias external_webcenter_custom_public_key -file external_
webcenter_custom_public_key.cer -keystore webcenter.jks -storepass welcome1
```

When prompted to trust the certificate, say yes.

Copy `webcenter.jks` to your `domain_home/config/fmwconfig` directory,
`bpel.jks` to your `SOA1_domain_home/config/fmwconfig` directory,
`soa_server3.jks` to your `SOA_2_domain_home/config/fmwconfig` directory,
`producer.jks` to your `External_Portlet_domain_home/config/fmwconfig`
directory, and `external_webcenter_custom.jks` to your
`External_WebCenter_domain_home/config/fmwconfig` directory.

Configure the WebCenter Portal Domain Keystore

Follow the steps below to configure the service instance reference for the WebCenter Portal domain:

1. Navigate to the `<DOMAIN_HOME>/config/fmwconfig` directory.
2. Copy `webcenter.jks` to the `<DOMAIN_HOME>/config/fmwconfig` directory if you haven't already done so.
3. Open `jps-config.xml` in an editor.
4. Locate `<serviceInstance` node for `keystore.provider Provider`.
5. Specify the location as `./webcenter.jks`.
6. Using WLST, connect to the WebCenter Portal domain as an administrator and run the following commands:

```
updateCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password="welcome1", desc="Keystore key")
updateCred(map="oracle.wsm.security", key="enc-csf-key", user="webcenter",
password="welcome1", desc="Encryption key")
updateCred(map="oracle.wsm.security", key="sign-csf-key", user="webcenter",
password="welcome1", desc="Signing key")
```

Configure the External Discussions Server Domain Keystore

Follow the steps below to configure the service instance reference for the discussions server:

1. Navigate to the `<DOMAIN_HOME>/config/fmwconfig` directory.

2. Copy `webcenter.jks` to the `<DOMAIN_HOME>/config/fmwconfig` directory if you haven't already done so.
3. Open `jps-config.xml` in an editor.
4. Locate `<serviceInstance node for keystore.provider Provider`.
5. Specify the location as `./owc_discussions.jks`.
6. Using WLST, connect to the WebCenter Portal domain as an administrator and run the following commands:

```
updateCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password="welcome1", desc="Keystore key")
updateCred(map="oracle.wsm.security", key="enc-csf-key",
user="owc_discussions", password="welcome1", desc="Encryption key")
updateCred(map="oracle.wsm.security", key="sign-csf-key",
user="owc_discussions", password="welcome1", desc="Signing key")
```

Configure the SOA1 Domain Keystore

Follow the steps below to configure the service instance reference for the SOA1 domain:

1. Navigate to the `<DOMAIN_HOME>/config/fmwconfig` directory.
2. Copy `bpel.jks` to the `<DOMAIN_HOME>/config/fmwconfig` directory if you haven't done already done so.
3. Open `jps-config.xml` in an editor.
4. Locate `<serviceInstance node for keystore.provider Provider`.
5. Specify the location as `./bpel.jks`.
6. Using WLST, connect to the SOA1 domain as an admin user and run the following commands:

```
updateCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password="welcome1", desc="Keystore key")
updateCred(map="oracle.wsm.security", key="enc-csf-key", user="bpel",
password="welcome1", desc="Encryption key")
updateCred(map="oracle.wsm.security", key="sign-csf-key", user="bpel",
password="welcome1", desc="Signing key")
```

Configure the SOA2 Domain Keystore

Follow the steps below to configure the service instance reference for the SOA2 domain:

1. Navigate to the `<DOMAIN_HOME>/config/fmwconfig` directory.
2. Copy `soa_server3.jks` to the `<DOMAIN_HOME>/config/fmwconfig` directory if you haven't done already done so.
3. Open `jps-config.xml` in an editor.
4. Locate `<serviceInstance node for keystore.provider Provider`.
5. Specify the location as `./soa_server3.jks`.
6. Using WLST, connect to the SOA2 domain as an admin user and run the following commands:

```
updateCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password="welcome1", desc="Keystore key")
updateCred(map="oracle.wsm.security", key="enc-csf-key", user="soa_server3",
```

```
password="welcome1", desc="Encryption key")
updateCred(map="oracle.wsm.security", key="sign-csf-key", user="soa_server3",
password="welcome1", desc="Signing key")
```

Configure the External Portlet Producer Domain Keystore

Follow the steps below to configure the service instance reference for the External Portlet Producer and External WebCenter Portal domain keystores:

1. Navigate to the <DOMAIN_HOME>/config/fmwconfig directory of the External Portlet Producer domain.
2. Copy producer.jks to the <DOMAIN_HOME>/config/fmwconfig directory if you haven't done already done so.
3. Open jps-config.xml in an editor.
4. Locate <serviceInstance node for keystore.provider Provider.
5. Specify the location as ./producer.jks.
6. Using WLST, connect to the External Portlet Producer domain as an administrator and run the following commands:

```
updateCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password="welcome1", desc="Keystore key")
updateCred(map="oracle.wsm.security", key="enc-csf-key", user="producer",
password="welcome1", desc="Encryption key")
updateCred(map="oracle.wsm.security", key="sign-csf-key", user="producer",
password="welcome1", desc="Signing key")
```

7. Navigate to the <DOMAIN_HOME>/config/fmwconfig directory of the External WebCenter Portal domain.
8. Copy producer.jks to the <DOMAIN_HOME>/config/fmwconfig directory if you haven't done already done so.
9. Open jps-config.xml in an editor.
10. Locate <serviceInstance node for keystore.provider Provider.
11. Specify the location as ./external_webcenter_custom.jks.
12. Using WLST, connect to the External Portlet Producer domain as an administrator and run the following commands:

```
updateCred(map="oracle.wsm.security", key="keystore-csf-key", user="owsm",
password="welcome1", desc="Keystore key")
updateCred(map="oracle.wsm.security", key="enc-csf-key",
user="external_webcenter_custom", password="welcome1", desc="Encryption key")
updateCred(map="oracle.wsm.security", key="sign-csf-key",
user="external_webcenter_custom", password="welcome1", desc="Signing key")
```

Configure the Discussions Server Connection

Supply the WS-Security client certificate information within the discussions server connection that is configured for Spaces or your Framework application, as described in [Section 14.3, "Registering Discussions Servers."](#) Also see [Section 34.3.3.4, "Configuring the Discussions Server Connection Settings"](#) for example connection detail settings for the Edit Discussions and Announcement Connection page.

34.4 Securing Spaces for Applications Consuming Spaces Client APIs with WS-Security

This section describes the administrator tasks required to configure WS-Security for Spaces so that the communication between the an application exposing Spaces APIs (the consumer) and Spaces (the producer) is secure, and that the identity of the user invoking the APIs is protected.

For information about the developer tasks for developing applications that consume Spaces client APIs, see "How to Set Up Your Framework application to Use the WebCenter Spaces APIs" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

This section includes the following subsections:

- [Section 34.4.1, "Configuring a Simple Topology for Applications Consuming Spaces Client APIs"](#)
- [Section 34.4.2, "Configuring a Typical Topology for Applications Consuming Spaces Client APIs"](#)
- [Section 34.4.3, "Configuring a Complex Topology for Applications Consuming Spaces Client APIs"](#)

34.4.1 Configuring a Simple Topology for Applications Consuming Spaces Client APIs

If your client application is part of the same domain as Spaces, you only need to specify the following for the `GroupSpaceWSContext()`:

```
GroupSpaceWSContext context = new GroupSpaceWSContext();
context.setRecipientKeyAlias("orakey");
```

If your client application is JDeveloper and you have access to the Spaces server's configured keystore, copy the same keystore to JDeveloper's `DefaultDomain/config/fmwconfig/dir` and configure the JDeveloper domain to use this keystore. The steps here would be exactly same as those in [Section 34.1.2.2, "Configuring the Keystore with WLST"](#), and you would then also need to specify the following on your client stub:

```
GroupSpaceWSContext context = new GroupSpaceWSContext();
context.setRecipientKeyAlias("orakey");
```

34.4.2 Configuring a Typical Topology for Applications Consuming Spaces Client APIs

If your client application is part of the same domain as Spaces, you only need to specify the following for the `GroupSpaceWSContext()`:

```
GroupSpaceWSContext context = new GroupSpaceWSContext();
context.setRecipientKeyAlias("webcenter");
```

If your client application is JDeveloper and you have access to the Spaces server's configured keystore, copy the same keystore to JDeveloper's `DefaultDomain/config/fmwconfig/dir` and configure the JDeveloper domain to use this keystore. The steps here would be exactly same as those in [Section 34.2.2.2, "Configuring the Keystore Using WLST"](#), and you would then also need to specify the following on your client stub:

```
GroupSpaceWSContext context = new GroupSpaceWSContext();
context.setRecipientKeyAlias("webcenter");
```

34.4.3 Configuring a Complex Topology for Applications Consuming Spaces Client APIs

If your client application is part of the same domain as Spaces, you only need to specify the following for the `GroupSpaceWSContext()`:

```
GroupSpaceWSContext context = new GroupSpaceWSContext();  
context.setRecipientKeyAlias("webcenter");
```

If your client application is JDeveloper, copy the same keystore to JDeveloper's `DefaultDomain/config/fmwconfig/dir` and configure the JDeveloper domain to use this keystore. The steps here would be exactly same as those in [Section 34.3.2.2, "Configuring the Keystore Using WLST"](#), and you would then also need to specify the following on your client stub:

```
GroupSpaceWSContext context = new GroupSpaceWSContext();  
context.setRecipientKeyAlias("webcenter");
```

Configuring Security for Portlet Producers

This chapter describes how to configure your WebCenter Portal application to handle security for WSRP and JPDK portlet producers.

This chapter includes the following sections:

- [Section 35.1, "Securing a WSRP Producer"](#)
- [Section 35.2, "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."](#)

35.1 Securing a WSRP Producer

The following sections describe how to secure access to JSR-168 standards-based WSRP portlets from WebCenter Portal applications:

- [Section 35.1.1, "Deploying the Producer"](#)
- [Section 35.1.2, "Attaching a Policy to the Producer Endpoint"](#)
- [Section 35.1.3, "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 Portal*.

35.1.1 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 24.8, "Deploying Portlet Producer Applications."](#)

35.1.2 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 user's 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 four SAML token policies:

- WSS 1.0 SAML token Policy:

`wss10_saml_token_service_policy`

This policy authenticates users using credentials provided in SAML tokens in the WS-Security SOAP header. The credentials in the SAML token are authenticated against a SAML login module. This policy can be applied to any SOAP-based endpoint.

–

- WSS 1.0 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 SHA-1 hashing algorithm for message integrity.

- WSS 1.0 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.

- WSS 1.1 SAML token with message protection:

`wss11_saml_token_with_message_protection_service_policy`

This policy enforces message-level protection (that is, message integrity and message confidentiality) and SAML-based authentication for inbound SOAP requests in accordance with the WS-Security 1.1 standard. Messages are

protected using WS-Security's Basic 128 suite of symmetric 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. This policy can be attached to any SOAP-based endpoint.

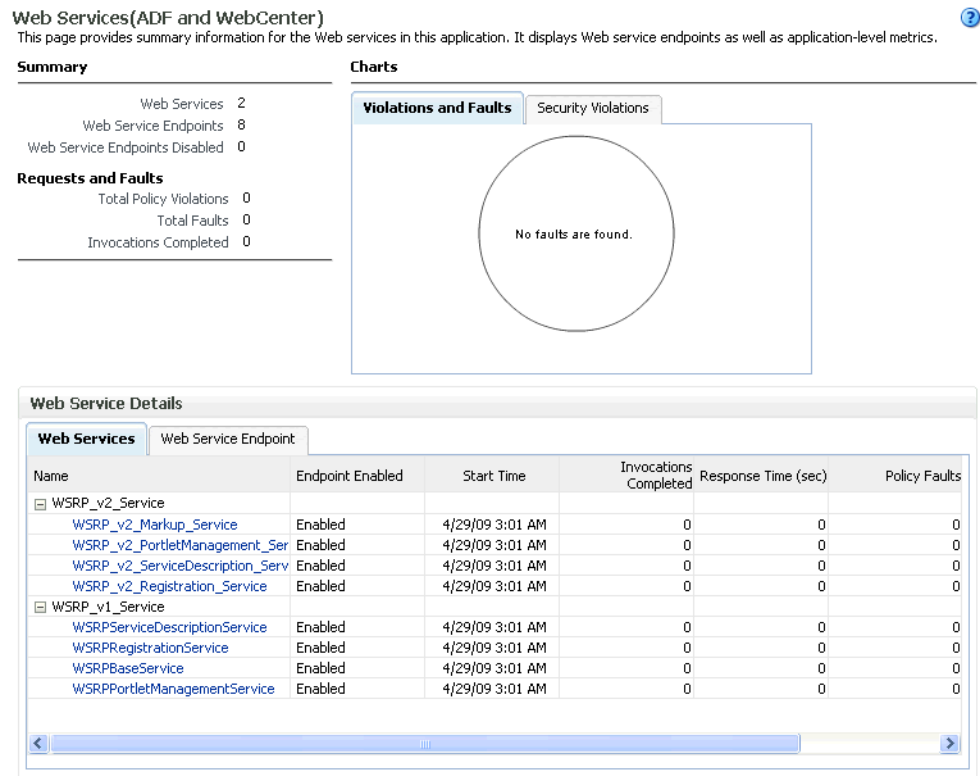
The keystore is configured through the security configuration. It extracts the SAML token from the WS-Security binary security token, and uses those credentials to validate users against the configured identity store.

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 35–1](#)).

Figure 35–1 Web Services 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 35–2).

Figure 35–2 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
 Style: document
 SOAP Version: soap1.1
 Stateful: False
 Implementation Type: JAX-RPC

Transport: HTTP
 Data Binding: jaxb20
 Legacy Configuration: False
 Implementation Class: WSRP_v2_Markup_Service
 WSDL Document: WSRP_v2_Markup_Service

Operation Name	One Way	Action	Input Encoding	Output Encoding	Invocations Completed	Execution Time Average (ms)
getMarkup	False	urn:oasis:names:tc:w	document	document	0	0
performBlockingInter	False	urn:oasis:names:tc:w	document	document	0	0
getResource	False	urn:oasis:names:tc:w	document	document	0	0
initCookie	False	urn:oasis:names:tc:w	document	document	0	0
handleEvents	False	urn:oasis:names:tc:w	document	document	0	0
releaseSessions	False	urn:oasis:names:tc:w	document	document	0	0

- Open the Policies tab to display the currently attached policies for the producer (see Figure 35–3).

Figure 35–3 Web Services Endpoint Policies 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
 Style: document
 SOAP Version: soap1.1
 Stateful: False
 Implementation Type: JAX-RPC

Transport: HTTP
 Data Binding: jaxb20
 Legacy Configuration: False
 Implementation Class: WSRP_v2_Markup_Service
 WSDL Document: WSRP_v2_Markup_Service

Policy Name	Category	Policy Reference Status	Total Violations	Security Viol	
				Authentication	Authorization
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 35-4](#)).

Figure 35-4 Attach/Detach Policies Page

Web Services > Web Service Endpoint > Attach Policies

Attach/Detach Policies(WSRP_v2_Markup_Service)

Attached Policies

Name	Category	Enabled	Description	View Full Description
No rows yet				

Available Policies

Search Category

Name	Category	Enabled	Description	View Full Description
oracle/wsaddr_policy	WS-Addressing	✓	This policy causes the pla...	<input type="button" value="View Full Description"/>
oracle/log_policy	Management	✓	This policy causes the req...	<input type="button" value="View Full Description"/>
oracle/wsmtom_policy	MTOM Attachm	✓	This Message Transmission ...	<input type="button" value="View Full Description"/>
oracle/binding_authorization_denyall_policy	Security	✓	This policy is a special c...	<input type="button" value="View Full Description"/>
oracle/binding_authorization_permitall_policy	Security	✓	This policy is a special c...	<input type="button" value="View Full Description"/>
oracle/binding_permission_authorization_policy	Security	✓	This policy is a special c...	<input type="button" value="View Full Description"/>
oracle/wss10_message_protection_service_policy	Security	✓	This policy enforces messa...	<input type="button" value="View Full Description"/>
oracle/wss10_saml_hok_token_with_message_protection_service_policy	Security	✓	This policy enforces messa...	<input type="button" value="View Full Description"/>
oracle/wss10_saml_token_service_policy	Security	✓	This policy authenticates ...	<input type="button" value="View Full Description"/>
oracle/wss10_saml_token_with_message_integrity_service_policy	Security	✓	This policy enforces messa...	<input type="button" value="View Full Description"/>
oracle/wss10_saml_token_with_message_protection_service_policy	Security	✓	This policy enforces messa...	<input type="button" value="View Full Description"/>
oracle/wss10_saml_token_with_message_protection_ski_basic256_service_	Security	✓	This policy enforces messa...	<input type="button" value="View Full Description"/>
oracle/wss10_username_id_propagation_with_msg_protection_service_poli	Security	✓	This policy enforces messa...	<input type="button" value="View Full Description"/>

- 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 35-5](#)).

Figure 35–5 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 Category 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

- When finished adding polices to attach to the producer endpoint, click **OK**.

35.1.3 Setting Up the Keystores

The steps to create and configure keystores for a WSRP producer depend on the topology of your WebCenter Portal environment, and are covered in the following sections:

- [Section 34.1, "Configuring WS-Security for a Simple Topology"](#)
- [Section 34.2, "Configuring WS-Security for a Typical Topology"](#)
- [Section 34.3, "Configuring WS-Security for a Complex Topology"](#)

Please refer to these sections for more complete instructions for setting up the keystores, and other WS-Security aspects of configuring WSRP producers.

35.2 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.
- 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 33.5, "Securing the Spaces Connection to Portlet Producers with SSL."](#)

35.2.1 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.

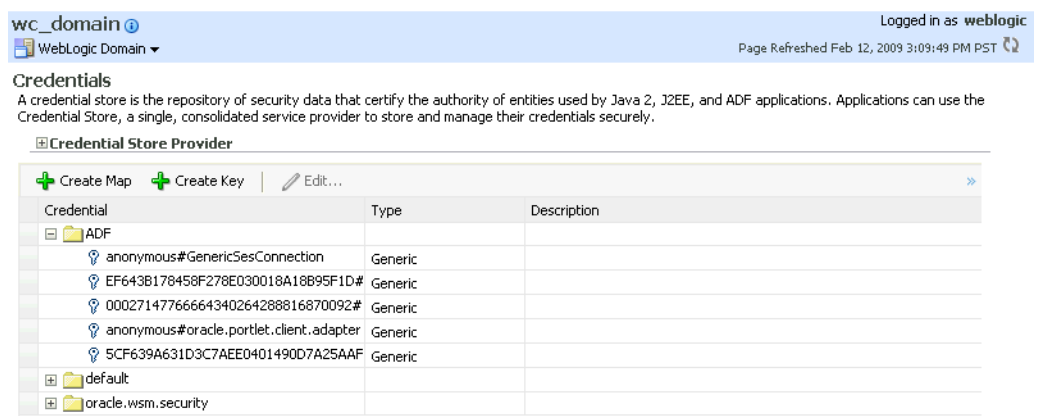
35.2.1.1 Defining a Shared Key Using Fusion Middleware Control

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**.

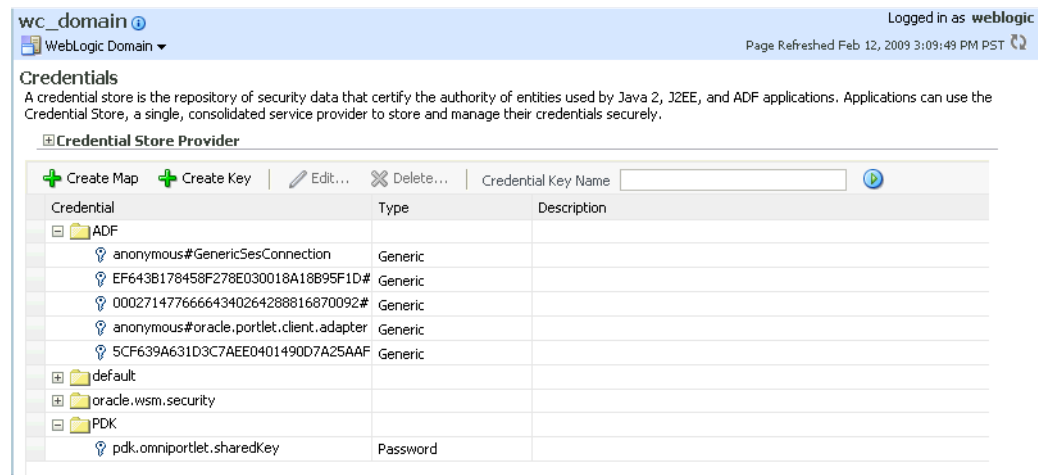
The Credentials pane displays (see [Figure 35–6](#)).

Figure 35–6 Credentials Pane



4. Click **Create Map** and enter PDK as the **Map Name** and click **OK**.
5. Click **Create Key** and select the map (PDK) 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>.sharedKey` (where `<service_id>` is the name of the producer), and a 10 to 20 hexadecimal digit **Password** and click **OK**.

The new key is displayed in the Credentials pane (see [Figure 35–7](#)).

Figure 35–7 Credentials Pane with New Shared Key

35.2.1.2 Defining a Shared Key Using WLST

You can also define a shared key using WLST:

1. Start WLST as described in [Section 1.13.3.1, "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='PDK', key='pdk.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='PDK', key='pdk.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.

Using WebCenter Portal Administration Console

This chapter provides information about the runtime administration console that is available for Framework applications. Framework applications are portal applications built in JDeveloper using WebCenter Portal: Framework.

This chapter includes the following sections:

- [Section 36.1, "Introduction to WebCenter Portal Administration Console"](#)
- [Section 36.2, "Accessing the WebCenter Portal Administration Console"](#)
- [Section 36.3, "Configuring Application Defaults"](#)
- [Section 36.4, "Managing Application Members and Roles"](#)
- [Section 36.5, "Managing Application Resources"](#)
- [Section 36.6, "Managing Services, Portlet Producers, and External Applications"](#)

Audience

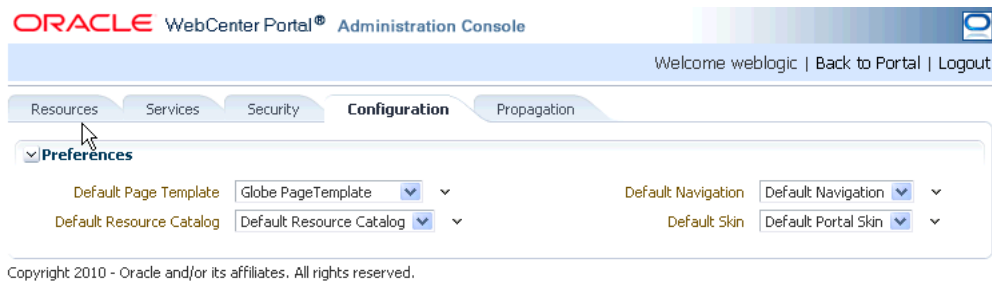
The content of this chapter is intended for users with the `Administrator` role who are responsible for managing users and roles, resources, and configuring default settings for Framework applications.

36.1 Introduction to WebCenter Portal Administration Console

By default, Framework applications offer several administration pages ([Figure 36-1](#)) that enable authenticated administrators to perform common administrative duties, including:

- Setting application-level preferences
- Managing users and granting application roles
- Managing and configuring application resources
- Managing content
- Managing and configuring portlet producers
- Managing and configuring external applications
- Creating and managing polls
- Propagating application updates

Figure 36–1 WebCenter Portal Administration Console



36.2 Accessing the WebCenter Portal Administration Console

To access the administration console for a Framework application:

1. Log in to your application as an administrator.

Initially, the WebCenter Portal Administration Console is only available to the system administrator. For information on how to grant the Administrator role to others, see [Section 36.4.3.3, "Giving a User Administrative Privileges."](#)

2. Do one of the following:
 - Click the **Administration** link ([Figure 36–2](#)).

Figure 36–2 WebCenter Portal Administration Console - Administration Link



- Access the WebCenter Portal Administration Console using the direct URL:

The default direct URL is:

```
http://www.server:port/context_root/admin
```

For example: `http://mycompany.com:8888/myapp/admin`

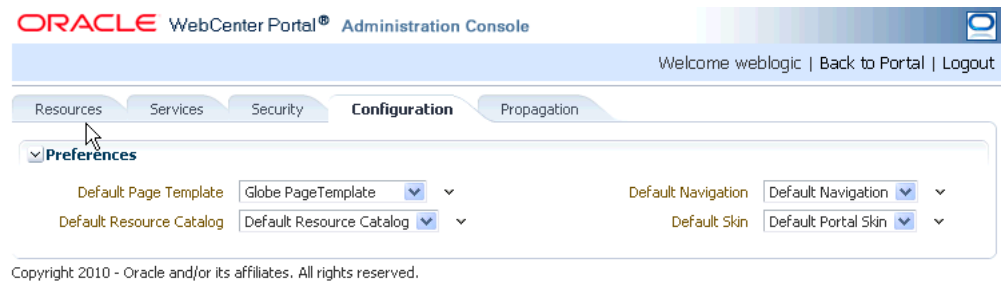
Application developers can, however, customize the direct URL using the `web.xml` entry:

```
<servlet-mapping>
  <servlet-name>PortalAdminServlet</servlet-name>
  <url-pattern>/admin</url-pattern>
</servlet-mapping>
```

The WebCenter Portal Administration Console displays (see [Figure 36–1](#)).

36.3 Configuring Application Defaults

On deployment, Framework applications are pre-configured with various default settings which administrators can customize to suit their audience through the WebCenter Portal Administration Console. From the Configuration tab ([Figure 36–3](#)), you can specify a default page template, skin, resource catalog, and navigation model.

Figure 36–3 WebCenter Portal Administration Console - Configuration Tab

This section includes the following subsections:

- [Section 36.3.1, "Choosing a Default Page Template"](#)
- [Section 36.3.2, "Choosing Default Resource Catalogs"](#)
- [Section 36.3.3, "Choosing a Default Navigation"](#)
- [Section 36.3.4, "Choosing a Default Skin"](#)
- [Section 36.3.5, "Choosing the Default Base Resource URL"](#)

36.3.1 Choosing a Default Page Template

In a Framework application, page templates define how individual pages and groups of pages display on a user's screen. Every page displays within a page template. For more information, see "Working with Page Templates" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

Administrators can define the default page template that is used to display pages.

To select a default page template for the application:

1. Navigate to the **Configuration** administration tab.
See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console"](#).

2. Choose a **Default Page Template** from the list provided.

The template you select is applied to existing pages and any new pages that are created.

Note: If users create pages and hard-code links to page templates, the **Default Page Template** has no effect.

3. Click **Apply**.

36.3.2 Choosing Default Resource Catalogs

In a Framework application, the resource catalog specifies a collection of elements, such as layout components, task flows, portlets, documents, and others, that authorized users can add to the application at runtime. For more information, see "Creating and Managing Resource Catalogs" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

To select a default resource catalog for the application:

1. Navigate to the **Configuration** administration tab.

See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console"](#).

2. Choose a **Default Resource Catalog** from the list provided.

The catalog you select is offered to users when they add content to pages, page templates, and so on.

3. Click **Apply**.

36.3.3 Choosing a Default Navigation

Navigations enable users to easily get around your Framework application and quickly access the information they need. For more information, see "Building a Navigation Model for Your Portal" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

Administrators can define the navigation used wherever there is a EL reference to `${navigationContext.defaultNavigation}`. This enables administrators to specify a default navigation model once and have it change throughout the system.

To choose a default navigation for the application:

1. Navigate to the **Configuration** administration tab.

See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console"](#).

2. Choose a **Default Navigation** from the list provided.

The navigation you select is applied wherever there is a EL reference to `${navigationContext.defaultNavigation}`.

Note: If users hard-code navigation model references (for example, in a parameter to a task flow), the **Default Navigation** has no effect.

3. Click **Apply**.

36.3.4 Choosing a Default Skin

Application administrators can customize the default appearance of a Framework application by changing its skin. A skin changes the way the user interface appears, but does not change the application's behavior.

To choose a default skin:

1. Navigate to the **Configuration** administration tab.

See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console"](#).

2. Choose a **Default Skin** from the list provided.

The skin you select is applied to all the pages in your application.

Note: The **Default Skin** has no effect on administration pages because the WebCenter Portal Administration Console uses an *internal skin* that does not change.

3. Click **Apply**.

36.3.5 Choosing the Default Base Resource URL

Developers can use EL expressions to dynamically generate the target URL for static resources. One way of doing this is to define a base URL preference to redirect resources to a desired server. With this option, EL expressions take a format that is illustrated by the following sample:

```
<af:image source="#{preferenceBean.baseResourceURL}/images/globe.png"/>
```

Administrators can configure the base URL at runtime in the Administration Console.

To choose the default base resource URL:

1. Navigate to the **Configuration** administration tab.
See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console"](#).
2. In the **Base Resource URL** field, enter the details for the server to use for static resources, using the following format:

```
protocol://serverName:serverPortcontextPath
```

For example:

```
http://myserver.com:7101/myFolder
```

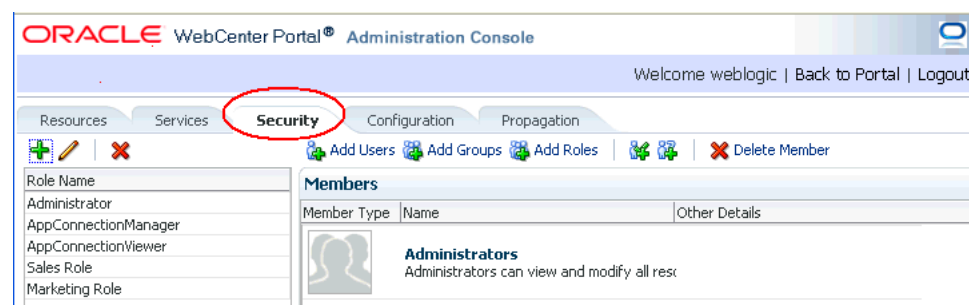
Tip: You can also use an EL expression that resolves to a valid server. For example, the default setting is:

```
#{request.scheme}://#{request.serverName}:#{request.serverPort}{request.contextPath}
```

36.4 Managing Application Members and Roles

Users who are granted the Administrator role, can manage application members and roles through the WebCenter Portal Administration Console. From the *Security* tab ([Figure 36-4](#)), you can add members, define roles, grant and revoke permissions and roles, as well as remove members.

Figure 36-4 WebCenter Portal Administration Console - Security Tab



This section contains the following subsections:

- [Section 36.4.1, "Understanding Users"](#)
- [Section 36.4.2, "Understanding Application Roles and Permissions"](#)
- [Section 36.4.3, "Managing Users"](#)
- [Section 36.4.4, "Managing Application Roles and Permissions"](#)

Note: The Security tab displays the *Role Manager* task flow, which can be added independently to any Framework application. For more information, see "Using the Role Manager Task Flow" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

36.4.1 Understanding Users

Framework application users each require a login account—provisioned directly from an existing identity store. Initially, only the Fusion Middleware Administrator (*weblogic* by default) can login and this default user has full administrative privileges through the Administrator role (see [Table 36-1](#)).

It is the Fusion Middleware Administrator's job to make individual users and user groups, who exist in the identity store, members of the WebCenter Portal and to assign each member an appropriate application role. Default and custom application roles are described in the section on [Section 36.4.2.1, "Understanding Application Roles."](#)

Alternatively, the Fusion Middleware Administrator may also choose to assign the application Administrator role to one or more other users and delegate this responsibility to others.

Table 36-1 Default Administrator for Framework Applications

User	Description
Fusion Middleware Administrator (<i>weblogic</i>)	Administrator for the entire WebCenter domain. This user can manage any application within the domain.

36.4.2 Understanding Application Roles and Permissions

Application roles control the level of access a user has to resources and services in a Framework application. This section describes application roles and permissions and includes the following subsections:

- [Section 36.4.2.1, "Understanding Application Roles"](#)
- [Section 36.4.2.2, "Understanding Application Permissions"](#)

36.4.2.1 Understanding Application Roles

Application role assignment is the responsibility of the application administrator. Administrators can assign members a default application role or create additional, custom roles specific to their application. For more detail, see:

- [Section 36.4.2.1.1, "Default Application Roles"](#)
- [Section 36.4.2.1.2, "Custom Application Roles"](#)
- [Section 36.4.2.2.1, "Application Permissions"](#)
- [Section 36.4.2.2.2, "Discussion Server Role Mapping"](#)
- [Section 36.4.2.2.3, "Understanding Enterprise Group Role Mapping"](#)

Application roles and permissions defined within a Framework application are stored in its *policy store* and, consequently, only apply to the application and do not imply any other permissions within the WebCenter Portal domain or other domains. Enterprise roles are different; enterprise roles are stored within the application's identity store and do not imply any permissions within the application.

36.4.2.1.1 Default Application Roles

Framework applications provide several default application roles that cannot be deleted (Table 36–2).

Table 36–2 Default Roles for a Framework Application

Application Role	Description
Administrator	<p>Users with the Administrator role can set application-wide preferences, manage resources, configure the content repository, create polls, and register producers and external applications.</p> <p>Administrators can also manage users and roles for the application, and delegate or revoke privileges to/from other users.</p> <p>Initially, the Administrators enterprise group is the only member assigned full administrative privileges through the Administrator role. This means that any user in the Administrators group has full administrative privileges in the Framework application.</p>
AppConnectionManager	<p>Users with this role can manage (<i>create</i>, <i>update</i>, and <i>delete</i>) portlet producers and external applications through corresponding task flows.</p> <p>Initially, only users with the Administrator role is a member of the AppConnectionManager role.</p>
AppConnectionViewer	<p>Users with this role can <i>view</i> portlet producers and external applications through corresponding task flows..</p> <p>Initially, any user who is logged in (that is, has <code>authenticated-role</code>) is a member of the AppConnectionViewer role.</p> <p>No direct permissions are granted to the AppConnectionViewer role so everything granted to <code>authenticated-role</code> is available to members with this role.</p>
authenticated-role	<p>Authenticated users are granted the <code>authenticated-role</code>—a standard OPSS (Oracle Platform Security Services) application role.</p>
anonymous-role	<p>Anyone who can access the application but is not logged in, is granted the <code>anonymous-role</code>—a standard OPSS (Oracle Platform Security Services) application role. Such users are anonymous, unidentified, and can see public content only.</p>

36.4.2.1.2 Custom Application Roles

Custom application roles (sometimes known as user-defined roles) are specific to your Framework application. When setting up the application, it is the 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 users, see [Section 36.4.4.1, "Defining Application Roles."](#)

36.4.2.2 Understanding Application Permissions

Every application role has specific, defined capabilities known as permissions. These permissions allow individuals to perform specific actions within the application. Note that no permission, inherits privileges from other permissions.

This section contains the following subsections:

- [Section 36.4.2.2.1, "Application Permissions"](#)
- [Section 36.4.2.2.2, "Discussion Server Role Mapping"](#)
- [Section 36.4.2.2.3, "Understanding Enterprise Group Role Mapping"](#)

36.4.2.2.1 Application Permissions

Permissions are categorized as follows and listed individually in the [Table 36–3](#):

- Application
- Mashup Styles
- Content Presenter Templates
- Skins
- Task Flows
- Resource Catalogs
- Page Styles
- Data Controls
- Navigations
- Page Templates
- Pages
- Links
- Lists
- People Connections

No permission, except for *Manage*, inherits privileges from other permissions.

Table 36–3 Application Permissions in Framework Applications

Category	Application Permissions
Application	<p>Manage - Enables access to all <i>WebCenter Spaces Administration</i> pages: Resources, Services, Security, Configuration, Propagation. Through these pages, users can manage application security (users/roles), configure application-wide properties and services, manage application resources, create and manage pages, and propagate application changes.</p> <p>Configuration - Enables users to view and perform operations on the Configuration tab.</p> <p>Propagation - Enables users to view and perform operations on the Propagation tab.</p>
Mashup Styles	<p>Create, Edit, and Delete - Create, edit and delete mashup styles for the application using the WebCenter Portal Administration Console (Resources tab).</p> <p>Create - Create mashup styles for the application.</p> <p>Edit - Edit mashup styles.</p> <p>See also, Chapter 36.5, "Managing Application Resources".</p>

Table 36-3 (Cont.) Application Permissions in Framework Applications

Category	Application Permissions
Content Presenter Templates	<p>Create, Edit, and Delete - Create, edit and delete content display templates for the application using the WebCenter Portal Administration Console (Resources tab).</p> <p>Create - Create content display templates for the application.</p> <p>Edit - Edit application-level content display templates.</p> <p>See also, Chapter 36.5, "Managing Application Resources".</p>
Skins	<p>Create, Edit, and Delete - Create, edit and delete skins using the WebCenter Portal Administration Console (Resources tab).</p> <p>Create - Create skins for the application.</p> <p>Edit - Edit skins.</p> <p>See also, Chapter 36.5, "Managing Application Resources".</p>
Task Flows	<p>Create, Edit, and Delete - Create, edit and delete task flows based on a mashup style using the WebCenter Portal Administration Console (Resources tab).</p> <p>Create - Create task flows for the application.</p> <p>Edit - Edit task flows.</p> <p>See also, Chapter 36.5, "Managing Application Resources".</p>
Resource Catalogs	<p>Create, Edit, and Delete - Create, edit and delete resource catalogs for the application using the WebCenter Portal Administration Console (Resources tab).</p> <p>Create - Create resource catalogs for the application.</p> <p>Edit - Edit resource catalogs.</p> <p>See also, Chapter 36.5, "Managing Application Resources".</p>
Page Styles	<p>Create, Edit, and Delete - Create, edit and delete page styles using the WebCenter Portal Administration Console (Resources tab).</p> <p>Create - Create page styles for the application.</p> <p>Edit - Edit page styles.</p> <p>See also, Chapter 36.5, "Managing Application Resources".</p>
Data Controls	<p>Create, Edit, and Delete - Create, edit and delete data controls for the application using the WebCenter Portal Administration Console (Resources tab).</p> <p>Create - Create data controls for the application.</p> <p>Edit - Edit data controls.</p> <p>See also, Chapter 36.5, "Managing Application Resources".</p>
Navigations	<p>Create, Edit, and Delete - Create, edit and delete navigations for the application using the WebCenter Portal Administration Console (Resources tab).</p> <p>Create - Create navigations for the application.</p> <p>Edit - Edit navigations.</p> <p>See also, Chapter 36.5, "Managing Application Resources".</p>
Page Templates	<p>Create, Edit, and Delete - Create, edit and delete page templates using the WebCenter Portal Administration Console (Resources tab).</p> <p>Create - Create page templates for the application.</p> <p>Edit - Edit page templates.</p> <p>See also, Chapter 36.5, "Managing Application Resources".</p>

Table 36–3 (Cont.) Application Permissions in Framework Applications

Category	Application Permissions
Page Service	<p>Grant Page Access - Manage page security.</p> <p>Edit - Add or edit page content, rearrange content, and set page parameters and properties.</p> <p>Customize - Customize pages for everyone.</p> <p>Personalize - Personalize your view of pages by adding, editing, or removing content.</p> <p>View - View pages.</p>
Links	<p>Create, and Delete - Create and delete links between objects, and manage link permissions.</p> <p>Delete - Delete a link between two objects.</p> <p>Create - Create links between objects.</p>
Lists	<p>Create, Edit, and Delete - Create, edit, and delete lists and list data.</p> <p>Create Lists - Create lists.</p> <p>Edit Lists - Edit list column definitions.</p> <p>Delete Lists - Delete any list.</p> <p>Edit List Data - Add, edit, and delete list data.</p> <p>View Lists - View lists and list data.</p>
People Connections	<p>Manage People Connections -Manage application-wide settings for People Connection services.</p> <p>Update People Connections Data -Edit content associated with People Connection services.</p> <p>Connect with People -Share content associated with People Connection services with others.</p>

36.4.2.2.2 Discussion Server Role Mapping

Some WebCenter Portal services that need access to "remote" (back-end) resources also require role-mapping based authorization. That is, the roles that allow users to work with the Discussions service in a Framework application, must be mapped to corresponding roles on WebCenter Portal's discussions server.

A Framework application uses *application roles* to manage user permissions within the application. On the discussions server, a different set of roles and permissions apply.

Any user assigned the Discussions-Create Edit Delete permission in a Framework application is automatically added on the discussions server and assigned the Administrator role (on the discussions server) with Category Admin permissions. In Framework applications, the Administrator role is granted the Discussions-Create Edit Delete permission by default as shown in [Table 36–4](#).

Table 36–4 Discussions Server Roles and Permissions

Discussion Server Role	Discussion Server Permissions	Framework Application Equivalent Application Permission
Administrator	Category Admin	Discussions-Create, Edit, and Delete Create, read, update and delete sub categories, forums and topics inside the category for which permissions are granted.

36.4.2.3 Understanding Enterprise Group Role Mapping

You can assign individual users or multiple users in the same enterprise group to Framework application roles. Subsequent enterprise group updates in the back-end identity store are then automatically reflected in the Framework application. Initially, when you assign an enterprise group to a Framework application role, everyone in the enterprise group is granted that role. If someone moves out of the group, the role is revoked. If someone joins the group, they are granted the role.

For a Framework application to properly maintain enterprise group-to-role mappings, back-end servers, such as the discussions server and content server, must support enterprise groups too. WebCenter Portal's Discussion Server and WebCenter Content's Content Server versions provided with this release both support enterprise groups but previous versions may not.

36.4.3 Managing Users

Administrators must ensure that all application users have appropriate permissions. To get permissions, users must be granted membership to the application through an appropriate application role.

This section tells you how to add members and assign roles. It contains the following subsections:

- [Section 36.4.3.1, "Adding Members to Application Roles"](#)
- [Section 36.4.3.2, "Assigning a User to a Different Role"](#)
- [Section 36.4.3.3, "Giving a User Administrative Privileges"](#)
- [Section 36.4.3.4, "Revoking Application Roles"](#)
- [Section 36.4.3.5, "Adding or Removing Users"](#)

36.4.3.1 Adding Members to Application Roles

You can grant membership to individual users or multiple users in the same enterprise group through the Security tab. Any user or group defined in the identity store is eligible for membership, see also, [Section 29.4, "Adding Users to the Embedded LDAP Identity Store."](#)

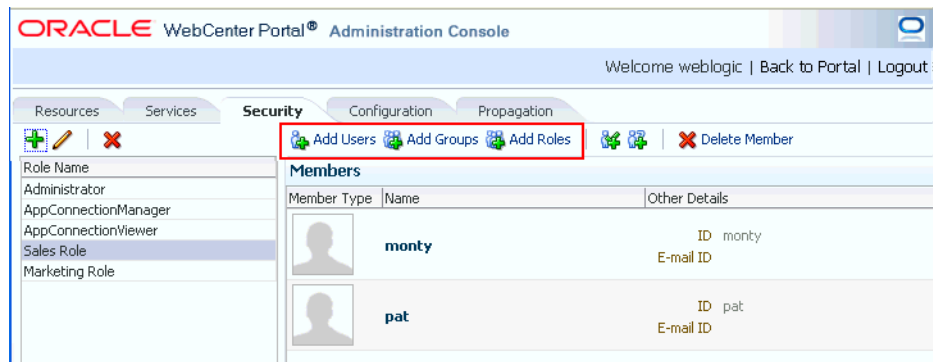
Updates in your back-end identity store, such as new users or someone leaving an enterprise group, are automatically reflected in the Framework application. Initially, when you assign an enterprise group to an application role, everyone in the group is granted that role. If someone moves out of the group, the role is revoked. If someone joins the group, they are granted the role.

Note: For a Framework application to properly maintain enterprise group-to-role mappings, back-end servers, such as the discussions server and content server, must support enterprise groups too. WebCenter Portal's Discussion server and Oracle WebCenter Content provided with WebCenter Portal 11.1.1.2.0 and later support enterprise groups but earlier versions may not.

To grant user membership through an appropriate application role:

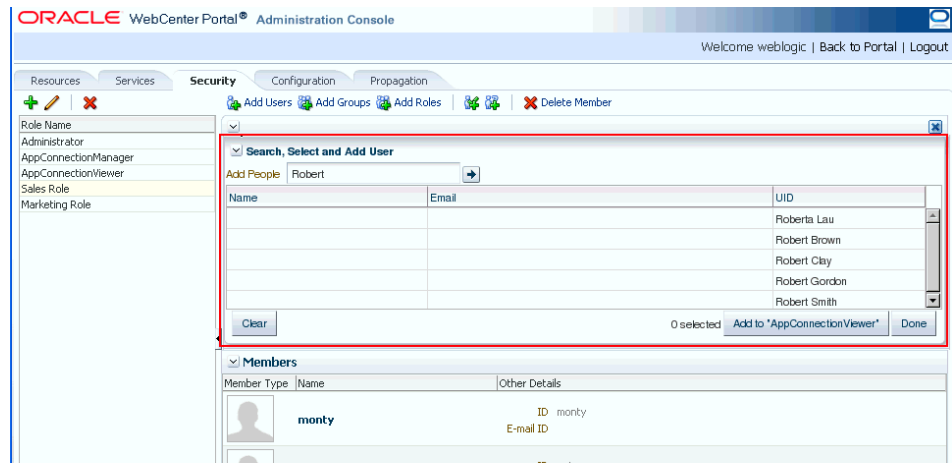
1. Navigate to the **Security** administration tab.
See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console"](#).
2. In the **Role Name** pane, select the role to assign to the user.
Notice that the current list of members assigned to the role you select are listed on the right (in the **Members** pane).
Only choose **Administrator** to assign full, administrative privileges for your application. If the role you want is not listed, create a new role that meets your requirements (see [Section 36.4.4.1, "Defining Application Roles"](#)).
3. Click **Add Users**, **Add Groups**, or **Add Roles** ([Figure 36–5](#)):
 - Add Users** - click to grant membership to individual users
 - Add Groups** - click to grant membership to everyone in a user group
 - Add Roles** - click to grant membership to everyone assigned to a particular application role

Figure 36–5 WebCenter Portal Administration Console - Add Members



4. If you know the exact name of the user, group, or application role, enter the name in the search box (**Add People**, **Add Group** or **Add Role**) and click the arrow icon. If you are not sure of the name you can search your identity store using part of the name as shown below (see [Figure 36–6](#)).

Figure 36–6 Add Users Pane - People Search

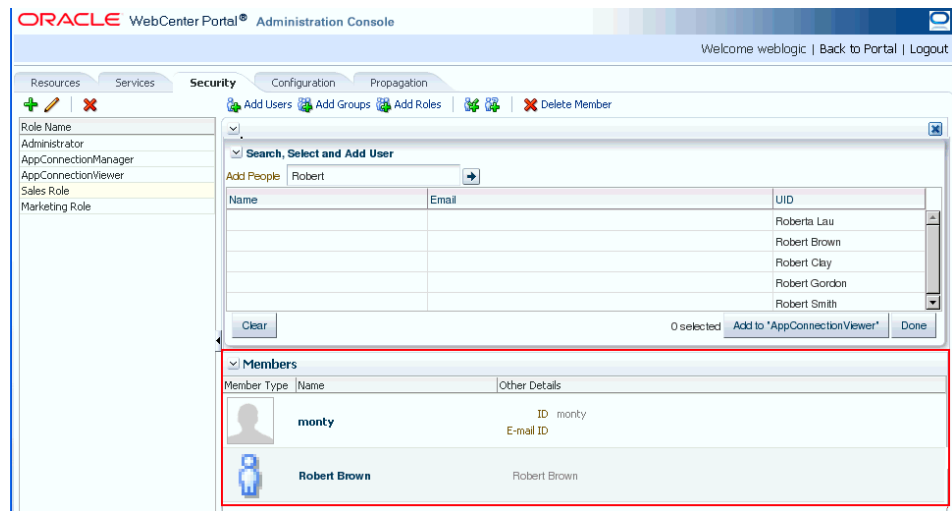


5. Select the user, group, or role to whom you want to grant the selected role, and click **Add to**. Use the Ctrl key to select multiple names.

Note: If the user, group, or role already has the role, directly or indirectly, the role is not granted; cyclic role assignments are not allowed.

The new members display in the Members pane (see [Figure 36–7](#)).

Figure 36–7 WebCenter Portal Administration Console - Members Pane



6. Click **Done** when finished.

36.4.3.2 Assigning a User to a Different Role

From time to time, a user's role in a Framework application may change. For example, a user may move out of sales into the finance department and in this instance, the user's role assignment may change from *Sales* to *Finance*. To change a user's role, first revoke membership for the user's previous role, then add the user to the new role. For more information see [Section 36.4.3.4, "Revoking Application Roles,"](#) and [Section 36.4.3.1, "Adding Members to Application Roles."](#)

Note: You cannot modify your own role or the Fusion Middleware Administrator's role. See [Section 36.4.2.1, "Understanding Application Roles"](#).

36.4.3.3 Giving a User Administrative Privileges

It's easy to give a user full, administrative privileges for your Framework application through the `Administrator` role. Administrators have the highest privilege level and can view and modify anything in the application so take care when assigning the `Administrator` role.

Most administrative tasks, such as managing users and roles, are exclusive to the `Administrator` role. See also, [Section 36.4.2.1.1, "Default Application Roles"](#).

36.4.3.4 Revoking Application Roles

It's easy to revoke application role assignments that no longer apply. Note, however, that revoking all of a user's application roles does not remove that user from the identity store.

Note: You cannot revoke your own role assignments or the Fusion Middleware Administrator's role. See [Section 36.4.2, "Understanding Application Roles and Permissions"](#).

To revoke application roles:

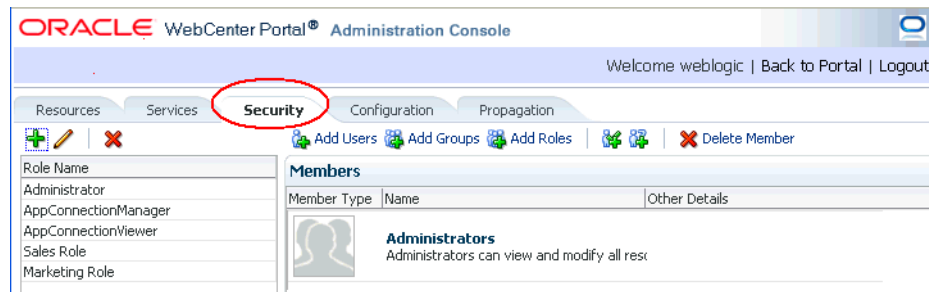
1. Navigate to the **Security** administration tab.
See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console"](#).
2. Select the role from the **Role Name** pane.
3. Select a user, group, or application role from the Members list.
4. Click **Delete Member**.
5. When prompted, click **Delete** to revoke the role for the user.

36.4.3.5 Adding or Removing Users

Administrators cannot add new user data directly to the Framework application's 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 29.4, "Adding Users to the Embedded LDAP Identity Store."](#)

36.4.4 Managing Application Roles and Permissions

Framework applications use application roles to manage permissions for users within the application. This section tells you how to manage application roles, and their permissions from the Security administration page ([Figure 36-8](#)).

Figure 36–8 WebCenter Portal Administration Console - Security Tab

Framework applications provide 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 36.4.2, "Understanding Application Roles and Permissions."](#)

This section contains the following subsections:

- [Section 36.4.4.1, "Defining Application Roles"](#)
- [Section 36.4.4.2, "Modifying Application Role Permissions"](#)
- [Section 36.4.4.3, "Granting or Removing Roles for Unauthenticated Users"](#)
- [Section 36.4.4.4, "Granting Roles to All Authenticated Users"](#)
- [Section 36.4.4.5, "Deleting Application Roles"](#)

36.4.4.1 Defining Application Roles

Use roles to characterize groups of application users and determine what they can see and do within their Framework application.

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.

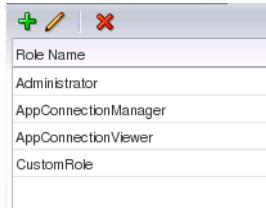
To define a new application role:

1. Navigate to the **Security** administration tab.
See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console"](#).
2. Click the **Add** icon (plus) above the Role Name pane.
The Create Role dialog displays ([Figure 36–9](#)).

Figure 36–9 WebCenter Portal Administration Console - Create Role Dialog

3. Enter a name and description for the new role, and click **Create Role**.
 Ensure the role name is self-descriptive. Make it as obvious as possible which users should belong to which roles. Role names can contain alphanumeric characters, blank spaces, @, and underscores.
 The new role is listed in the Roles pane (Figure 36–10).

Figure 36–10 WebCenter Portal Administration Console - Roles Pane



4. Continue by defining the user permissions for the role as described in [Section 36.4.4.2, "Modifying Application Role Permissions."](#)

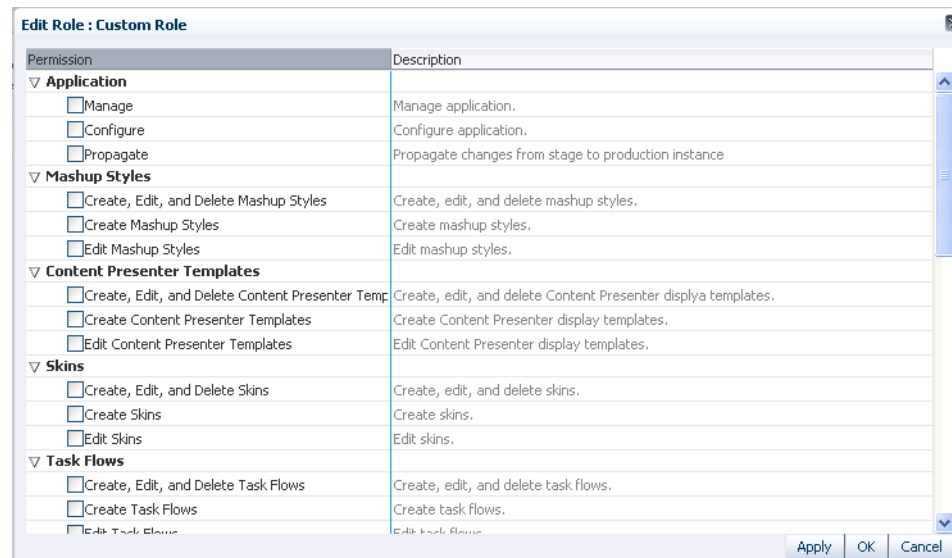
36.4.4.2 Modifying Application Role Permissions

Permissions should always be set after creating a new role, but administrators can modify the permissions associated with an application role at any time.

Application role permissions allow individuals to perform specific actions within their application. Application permissions are described in [Section 36.4.2, "Understanding Application Roles and Permissions."](#)

To change the permissions assigned to a role:

1. Navigate to the **Security** administration tab.
 See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console"](#).
2. Select the role for which to view or modify permissions, and click the **Edit** icon (pencil).
 The Edit Role dialog displays with the current permissions for the role ([Figure 36–11](#)).

Figure 36–11 WebCenter Portal Administration Console - Edit Role Dialog

3. Select or clear permissions check boxes to enable or disable permissions for the role.
4. Click **Apply** to save or **OK** to save and exit.

The new permissions are effective immediately.

36.4.4.3 Granting or Removing Roles for Unauthenticated Users

Anyone who is not logged in to a Framework application assumes the `anonymous-role`. Initially, users with the `anonymous-role` have no privileges and only see public application pages, such as the login or landing page, and also content that individual users choose to make public.

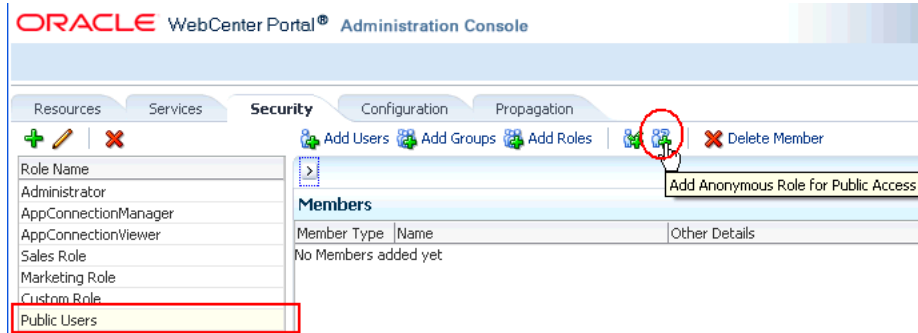
Caution: Take care when granting privileges to the `anonymous-role`. Avoid granting administrative privileges, or any permission that might be considered unnecessary. For security reasons, Oracle recommends that you limit what anonymous users can see and do in your application. If you have no public or anonymous access to your application, any grants that are currently given to `anonymous-role` should be removed or moved to `authenticated-role`.

To grant application roles to the public:

1. Navigate to the **Security** administration tab.
See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console"](#).
2. If you have not done so already, define a role that grants permissions suitable for unauthenticated users.
See also, [Section 36.4.4.1, "Defining Application Roles"](#).
3. Select the role that defines privileges suitable for unauthenticated users.

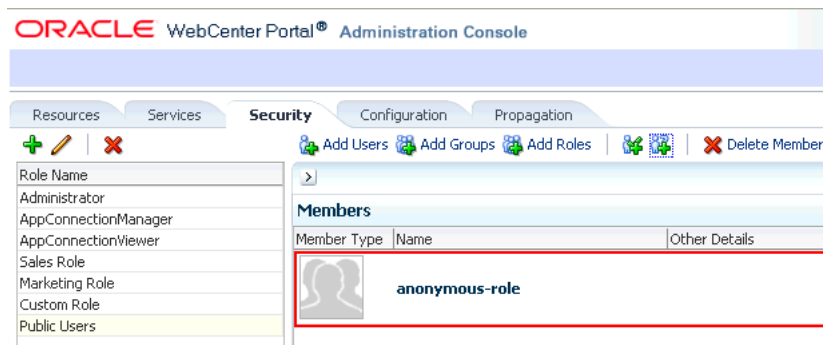
4. Click **Add Anonymous Role for Public Access** (Figure 36–12). (If the `anonymous-role` has already been added and you want to remove it, click **Delete**.)

Figure 36–12 WebCenter Portal Administration Console - Add Public Access



The anonymous-role is added to the members list (Figure 36–13).

Figure 36–13 WebCenter Portal Administration Console - Add Public Access



36.4.4.4 Granting Roles to All Authenticated Users

Anyone who is logged in to a Framework application assumes the `authenticated-role`.

Other important notes:

- The `authenticated-role` always inherits permissions from the `anonymous-role`
- Custom application roles all inherit permissions from the `authenticated-role`.

36.4.4.5 Deleting Application Roles

When an application role is no longer required you should remove it from your application. This helps maintain a valid role list, and prevents inappropriate role assignment. You cannot, however, delete a role that is granted to you, directly or indirectly.

Application roles are deleted even when users are still assigned to them.

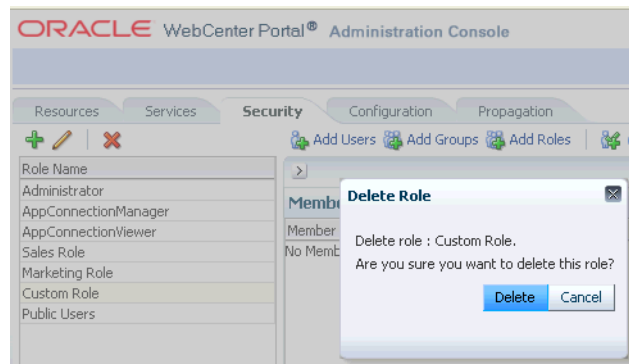
Note: Default roles cannot be deleted: Administrator, AppConnectionManager, AppConnectionViewer, authenticated-role, anonymous-role. See also, [Section 36.4.2.1.1, "Default Application Roles."](#)

As you cannot delete *default roles*, application users can log in through the authenticated-role, even when all other application roles are revoked.

To delete an application role:

1. Navigate to the **Security** administration tab.
See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console"](#).
2. Select the role to delete from the list of roles and click the **Delete** icon (x).

Figure 36–14 Deleting an Application Role

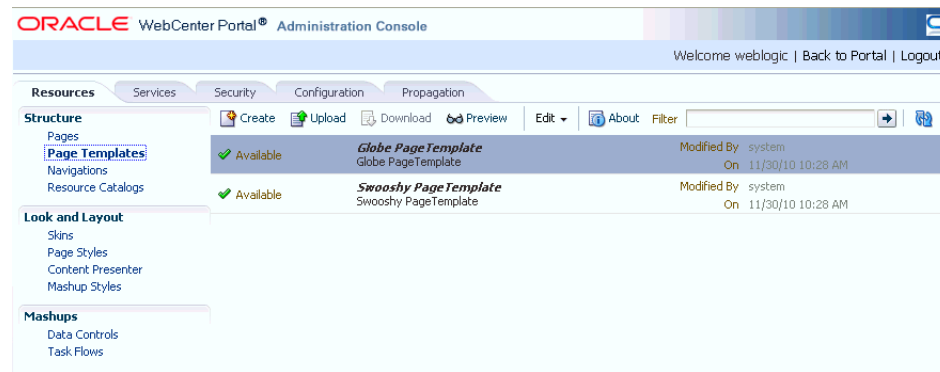


3. When prompted, click **Delete** to confirm that you want to delete the role.

The role is removed from the table. Users assigned to only this role can still log in through the authenticated-user role.

36.5 Managing Application Resources

By using the Resources page of the WebCenter Portal Administration Console, you can manage your application resources—pages, page templates, navigations, resource catalogs, skins, page styles, content presenter templates, mashup styles, data controls, and task flows ([Figure 36–15](#)). You can perform tasks such as create, edit, copy, publish, upload, and download your application resources. For information about various resources, see the section "Introducing Resources" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

Figure 36–15 WebCenter Portal Administration Console - Resources Page

This section includes the following subsections:

- [Section 36.5.1, "Working with Pages"](#)
- [Section 36.5.2, "Creating a Resource"](#)
- [Section 36.5.3, "Copying a Resource"](#)
- [Section 36.5.4, "Editing Resources"](#)
- [Section 36.5.5, "Setting Properties on a Resource"](#)
- [Section 36.5.6, "Showing or Hiding a Resource"](#)
- [Section 36.5.7, "Setting Resource Security"](#)
- [Section 36.5.8, "Downloading and Uploading a Resource"](#)
- [Section 36.5.9, "Previewing a Resource"](#)
- [Section 36.5.10, "Deleting a Resource"](#)

36.5.1 Working with Pages

At runtime, you can create and manage application pages.

This section includes the following subsections:

- [Section 36.5.1.1, "Creating a Page"](#)
- [Section 36.5.1.2, "Creating a Sub Page"](#)
- [Section 36.5.1.3, "Setting Page Access"](#)
- [Section 36.5.1.4, "Reordering a Page"](#)
- [Section 36.5.1.5, "Moving a Page in the Page Hierarchy"](#)
- [Section 36.5.1.6, "Renaming a Page"](#)

For information about editing, copying, or deleting a page, refer to the generic resource procedures documented later in this chapter.

36.5.1.1 Creating a Page

To create an application page at runtime:

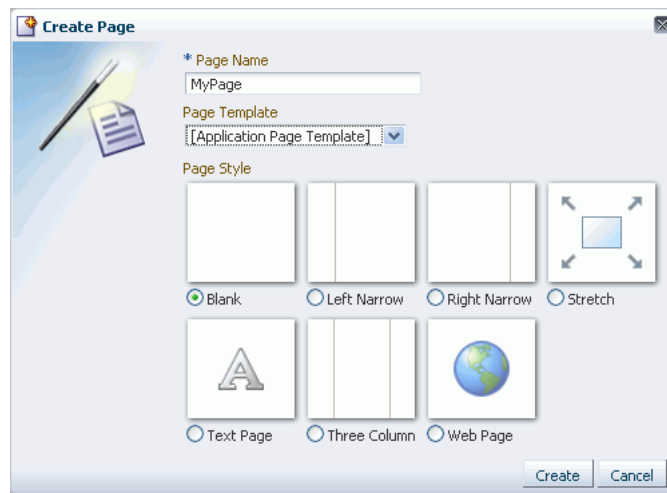
1. Open the **Resources** tab in WebCenter Portal Administration Console.
See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console."](#)
2. In the navigation panel on the left, click **Pages**.

3. On the menu bar, click **Create Page**.
4. In the **Create Page** dialog, in the **Page Name** field, enter the name of the page.
5. From the **Page Template** list, select the page template on which you want to base your page.

Note: If you do not specify a page template, the default template is used. It is recommended that you leave the **Page Template** list blank unless you want to override the default template.

6. From the **Page Style** list, select the style you want to use for your page.
- For information about page styles, see the "What You Should Know About Page Styles" section in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

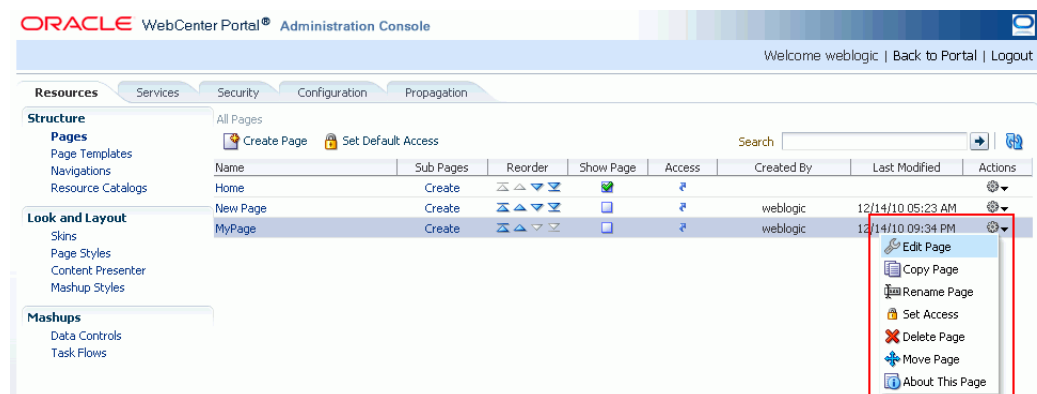
Figure 36–16 Creating a Page



7. Click **Create**.

The newly created page is listed on the Resources page. You can manage the page by using the options available on the **Actions** menu of the page (Figure 36–17).

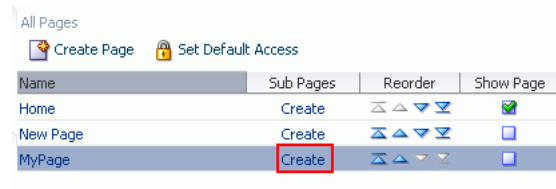
Figure 36–17 Actions Menu of a Page



36.5.1.2 Creating a Sub Page

The procedure to create a sub page is similar to creating a main page as described in [Section 36.5.1.1, "Creating a Page."](#) On the **Resources** page, you need to click **Create** next to the page for which you want to create a sub page ([Figure 36–18](#)). By default, sub pages inherit security from their parent page.

Figure 36–18 *Creating a Sub Page*

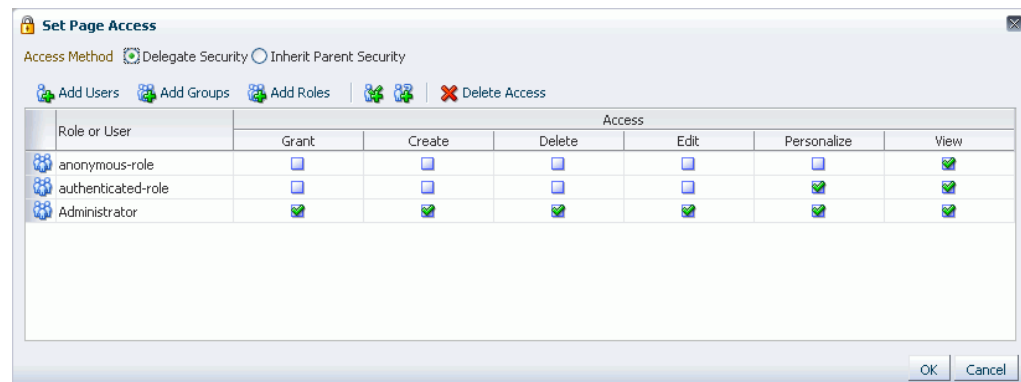


36.5.1.3 Setting Page Access

All your application pages reside under the root node, and by default, inherit the permissions defined for the root node. You can define custom permissions for the root node. Further, you can override the default root node permissions, and specify custom permissions for individual pages. By default, sub pages inherit security from their parent page.

While setting page access, you can choose either of these access methods: Delegate Security or Inherit Parent Security ([Figure 36–19](#)).

Figure 36–19 *Setting Page Access*



Choose:

- Delegate Security** - to define who may manage and update a page. When you select this option, all permissions that a page currently inherits from its parent are displayed in the dialog. This effectively is the current security policy applicable on the page. You can further refine the grants by adding new grants or removing the existing ones.
- Inherit Parent Security** - to inherit permissions defined for a page's parent node. When you set this option, any security permissions defined on the page are deleted, and the parent node's security settings take effect.

You can define the following page permission actions:

- Manage** - grants all other page permissions and is typically used for specifying a super administrator type of access. This permission action is available only when defining access on the root node.

- **Grant** - allows a user to further grant the access that they already have to other users, groups, or roles. For example, if a user has the Grant and Edit permissions, the user can further grant these two actions only; she cannot grant any other permission, like Delete or Personalize.
- **Create** - allows a user to create sub pages under the current page.
- **Delete** - allows a user to delete a page along with all its sub pages.
- **Edit** - allows a user to edit a page.
- **Personalize** - allows a user to personalize a page.
- **View** - allows a user to view a page.

All permissions follow one of the two permission models - delegation or containment. Delegation is when an entity has been granted a particular permission on a page, and this is all that is used to evaluate whether the entity has the said permission action or not. All permission actions other than View fall in this category. A permission is of containment type if the permission is granted to an entity on a page, as well as all the nodes up in the hierarchy where security is defined. Only the View permission action falls in this category.

So, to be able to view a page, you need to have the View permission action on the specified page and all nodes up in the hierarchy to the root node. If you do not have the View permission on an intermediate node in the page hierarchy, you cannot view the specified page. For other permission actions (delete, edit, and the like), you just need that particular permission on the page.

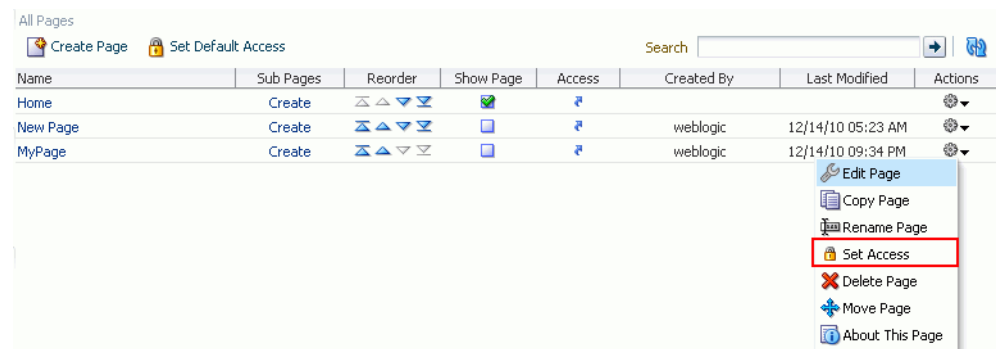
This section includes the following subsections:

- [Section 36.5.1.3.1, "Setting Permissions on an Individual Page"](#)
- [Section 36.5.1.3.2, "Setting Permissions on the Root Node"](#)

36.5.1.3.1 Setting Permissions on an Individual Page To set permissions on a specific page:

1. Navigate to the **Resources** page, as described in [Section 36.2, "Accessing the WebCenter Portal Administration Console."](#)
2. In the left navigation panel, click **Pages**.
3. From the list of pages, open the **Actions** menu for the required page, then select **Set Access**.

Figure 36–20 Setting Page Access



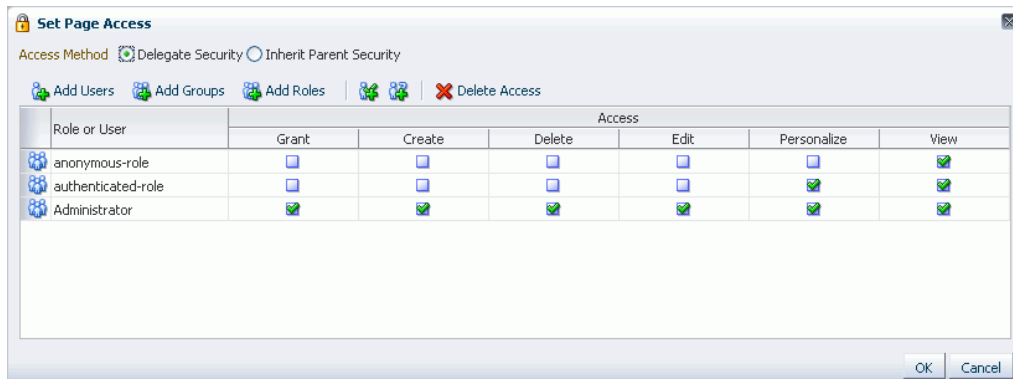
4. In the Set Page Access dialog, select an access method ([Figure 36–21](#)):

- Delegate Security**—Select this method to define who may manage and update this page node, and all its children in the hierarchy that have not overridden security. Selecting this method shows the default permissions available. You can further refine the permissions by adding new permissions or removing the existing ones.

If you select this option, proceed to step 5.

- Inherit Parent Security**—Select this method to inherit permissions defined for the page’s parent node. If you select this method, click **OK** to save your changes and exit the dialog.

Figure 36–21 Setting Page Access



- If you selected **Delegate Security**, specify the user, group, or role to which you want to grant access to the page.
 - Click **Add Users** to search for and select individual users included in your identity store. Select the required user(s), and click **OK**.
 - Click **Add Groups** to search for and select groups of users included in your identity store. Select the required group(s), and click **OK**.
 - Click **Add Roles** to search for and select the application roles to which you want to grant access to the page. Select the required role(s), and click **OK**.
- For each user, group, or role listed in the **Role or User** column, specify the level of access you want to grant. You can grant any of the following permissions: Grant, Create, Delete, Edit, Personalize, and View.
- Optionally, you can click the **Add Authenticated Role for Logged in User Access** icon to add **authenticated-role** and define the access for all authenticated users. You can click the **Add Anonymous Role for Public Access** icon to add **anonymous-role** and grant the required permissions to all users.
- If you want to revoke permissions from any user, group, or role, select that entity and click **Delete Access**.
- Click **OK** to save the security settings for the page.

The lock icon in the Access column for a page signifies that **Delegate Security** access method has been set for the page; the arrow icon signifies that **Inherit Parent Security** access method has been set for the page (Figure 36–22).

Figure 36–22 Access Methods Specified for Pages

Name	Sub Pages	Reorder	Show Page	Access	Created By	Last Modified	Actions
Home	Create	△ ▲ ▽ ▾	🗑️	🔒			⚙️
New Page	Create	△ ▲ ▽ ▾	🗑️	🔒	weblogic	12/14/10 05:23 AM	⚙️
MyPage	Create	△ ▲ ▽ ▾	🗑️	🔒	weblogic	12/14/10 09:34 PM	⚙️

36.5.1.3.2 Setting Permissions on the Root Node All page and sub page nodes that do not have security overridden, derive their access settings from the root node. You can define permissions for the root node by using the **Set Default Access** option on the **Pages** page on the **Resource** tab (Figure 36–23). The rest of the procedure is same as that for setting permissions for a specific page. For information, see [Section 36.5.1.3.1, "Setting Permissions on an Individual Page."](#)

When you set permissions for the root node, in addition to other permissions, you can also set the Manage permission. A user with this permission has complete access on the entire pages hierarchy irrespective of the settings on individual pages.

Figure 36–23 Setting Access for the Root Node

ORACLE WebCenter Portal® Administration Console

Resources Services Security Configuration Propagation

Structure

- Pages (Selected)
- Page Templates
- Navigations
- Resource Catalogs

Look and Layout

- Skins

Name	Sub Pages	Reorder
Home	Create	△ ▲ ▽ ▾
MyPage	Create	△ ▲ ▽ ▾
New Page	Create	△ ▲ ▽ ▾

36.5.1.4 Reordering a Page

You can reorder your pages. This order is used when you include pages in the navigation model through a Page Query.

To change the order of a page:

1. Navigate to the **Resources** page in WebCenter Portal Administration Console.
See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console."](#)
2. In the left navigation panel, click **Pages**.
3. Drag the page to the required location in the page hierarchy.

To reorder pages, you can also use the icons displayed in the Reorder column (Figure 36–24). Use the icons to move your page to the top of the list, bottom of the list, before the preceding page, or after the page displayed next in the list.

Figure 36–24 Reordering a Page

Name	Sub Pages	Reorder	Show Page
Home	Create	△ ▲ ▽ ▾	🗑️
New Page	Create	△ ▲ ▽ ▾	🗑️
MyPage	Create	△ ▲ ▽ ▾	🗑️

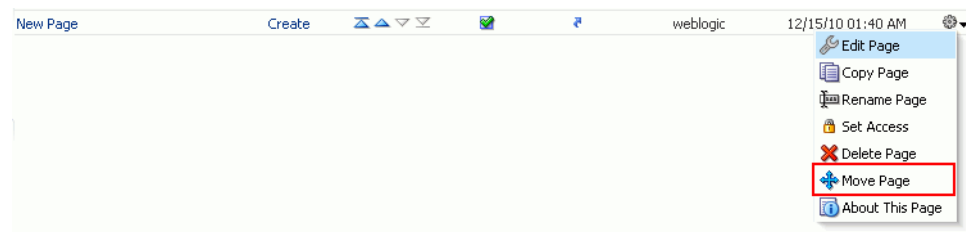
36.5.1.5 Moving a Page in the Page Hierarchy

You can change the level at which a page appears in the page hierarchy—you can move a page to appear as a sub page, appear at the root level, or appear as a parent page.

To move a page in the page hierarchy:

1. Navigate to the **Resources** page in WebCenter Portal Administration Console.
See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console."](#)
2. In the left navigation panel, click **Pages**.
3. Open the **Action** menu for the page that you want to move, and choose **Move Page** (Figure 36–25).

Figure 36–25 Actions Menu of a Page



4. In the Move Page dialog, select the level at which you want to move the page in the page hierarchy.

For example, if you want your page to appear as a sub page of **MyPage**, click **MyPage** (Figure 36–26).

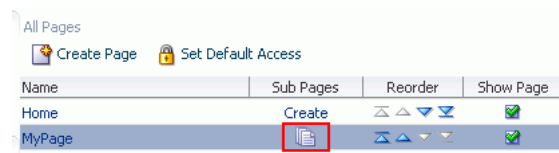
Figure 36–26 Moving a Page



5. Click **OK**.

In [Figure 36–27](#), the sub page icon in the **Sub Pages** column represents that **MyPage** now contains a sub page.

Figure 36–27 A Page Updated in the Page Hierarchy



36.5.1.6 Renaming a Page

To rename a page:

1. Navigate to the **Resources** page in WebCenter Portal Administration Console, as described in [Section 36.2, "Accessing the WebCenter Portal Administration Console."](#)
2. In the left navigation panel, click **Page**.
3. Open the **Action** menu for the page you want to rename, and choose **Rename Page**.
4. In the Rename Page dialog, enter the desired name.
5. Click **OK**.

36.5.2 Creating a Resource

Even after your application has been deployed, as an administrator, you may need to constantly update it to meet your organization's requirements. Framework applications enable you to create and edit resources at runtime, without requiring you to redeploy your application.

To create a resource:

Note: The procedure for creating a data control and a page is different than other resources. For information about how to create a data control, navigate to the **Resources** page in WebCenter Portal Administration Console and then follow the procedure outlined in the chapter "Creating and Managing Data Controls" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*. For information about creating a page, see [Section 36.5.1.1, "Creating a Page."](#)

1. Navigate to the **Resources** page in WebCenter Portal Administration Console. See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console."](#)
2. In the left navigation panel, select the category of the resource you want to create.
3. On the menu bar, click **Create**.
4. In the **Create** dialog, in the **Name** field, enter the name of the resource.
5. In the **Description** field, enter a description of the resource.
6. From the **Copy from** list, select the existing resource that you want to extend for creating a new resource.

Note: The **Copy from** list is available for page template, navigation, Resource Catalog, and skin resources. It is not available for a task flow resource.

For a task flow resource, you need to select a mashup style. For information, see the section "Creating a Task Flow" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

7. Click **Create**.

The newly created resource is listed on the Resources page. The gray icon next to a resource indicates that it is not yet published and hence not available to users for

use. For information about publishing resources, see [Section 36.5.6, "Showing or Hiding a Resource."](#)

36.5.3 Copying a Resource

You can create a copy of a resource. This feature is useful when you want to create a backup of a resource or update a resource while keeping the original in use. When you create a copy of a resource, the copy is marked as hidden.

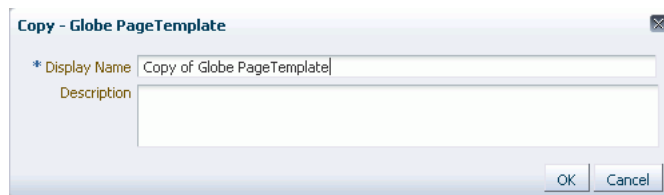
To make a copy of a resource:

1. Navigate to the **Resources** page in WebCenter Portal Administration Console.
See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console."](#)
2. In the left navigation panel, select the desired type of resource.
3. From the list of resources, select the resource you want to copy.
4. From the **Edit** menu, choose **Copy**.

Note: To make a copy of a page, select **Copy Page** from the **Actions** menu of the page. In the Copy Page dialog, specify the page name and click **OK**.

5. In the Copy dialog, in the **Display Name** field, enter a name for the resource copy ([Figure 36-28](#)).

Figure 36-28 Copying a Resource



6. In the **Description** field, enter a description of the resource copy.
7. Click **OK**.

36.5.4 Editing Resources

At runtime, you can perform two types of resource editing:

- Simple editing - provides a simple means of editing a resource's basic settings. Use the Edit dialog to perform simple editing.
- Source editing - enables you to work with the source code of a resource. Use the Edit Source dialog to perform source editing.

36.5.4.1 Editing the Source Code of a Resource

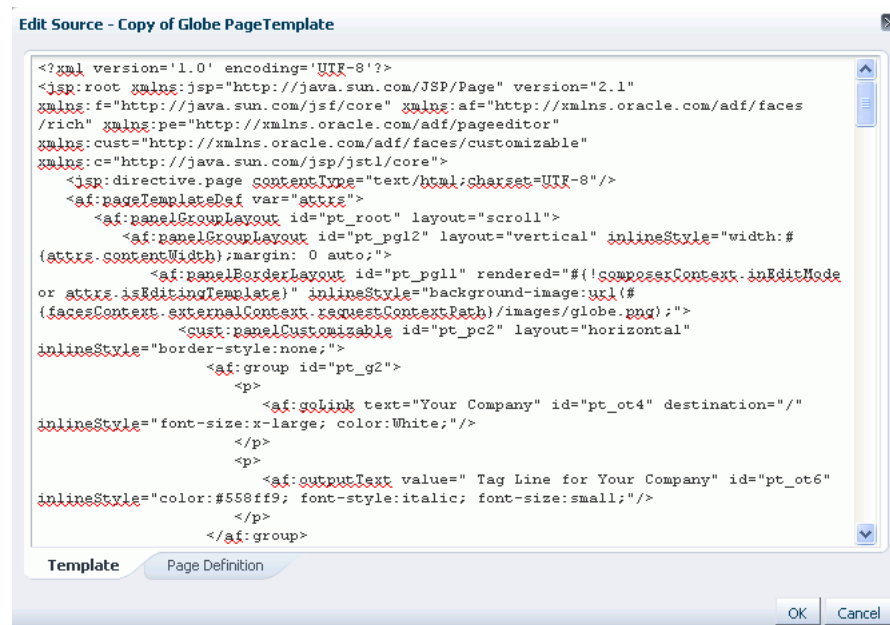
To get more control over resource editing at runtime, you can edit the underlying source code of any custom resource, except data controls and pages.

To edit the source code of a resource:

1. Navigate to the **Resources** page in WebCenter Portal Administration Console, as described in [Section 36.2, "Accessing the WebCenter Portal Administration Console."](#)
2. From the navigation panel on the left, select the desired type of resource.
3. From the list of resources displayed on the right, select the resource whose code you want to edit.
4. From the **Edit** menu, choose **Edit Source**.
The Edit Source dialog displays the resource definition.
5. Edit the code as required ([Figure 36–29](#)).

The XML syntax in the code is validated and an error message is displayed if you miss any tags or add them incorrectly. Validation is not performed for non-XML files, such as a CSS file.

Figure 36–29 Editing the Source of a Resource



6. Click **OK**.

36.5.4.2 Editing a Resource by Using the Edit Dialog

To edit a resource at runtime:

1. Navigate to the **Resources** page in WebCenter Portal Administration Console.
See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console."](#)
2. In the left navigation panel, select the desired type of resource.
3. From the list of resources, select the resource you want to edit.
4. From the **Edit** menu, choose **Edit**.

Note: To edit a page, select the **Edit Page** option from the **Actions** menu of the page.

5. Edit the resource as desired.

The properties that you can edit vary from resource to resource. For information about the properties of a resource that can be edited, refer to the relevant resource chapter listed in the table "Resources Available in Spaces" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*. The procedure to edit a resource in a Framework application is similar to that in the Spaces application.

36.5.5 Setting Properties on a Resource

Each resource has certain associated properties that define its display properties and attributes. Authorized users can edit these properties by using the Edit Properties dialog. For information about the properties displayed in the Edit Properties dialog, see the "What You Should Know About a Resource's Properties" section in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

This section describes how to access the Edit Properties dialog and set resource properties. It includes the following subsections:

Note: The properties described in this section are not applicable to a page resource.

- [Section 36.5.5.1, "Accessing the Edit Properties Dialog of a Resource"](#)
- [Section 36.5.5.2, "Renaming, Describing, and Categorizing a Resource"](#)
- [Section 36.5.5.3, "Associating an Icon with a Resource"](#)
- [Section 36.5.5.4, "Working with Attributes of a Resource"](#)

36.5.5.1 Accessing the Edit Properties Dialog of a Resource

To access the Edit Properties dialog of a resource:

1. Navigate to the **Resources** page in WebCenter Portal Administration Console, as described in [Section 36.2, "Accessing the WebCenter Portal Administration Console."](#)
2. From the left navigation panel, select the type of resource you want to edit.
3. Highlight the relevant resource, and choose **Edit Properties** from the **Edit** menu.

The Edit Properties dialog opens ([Figure 36–30](#)).

Figure 36–30 Edit Properties Dialog of a Resource

Edit Properties - Copy of Globe PageTem...

General

Display Name Copy of Globe PageTemplate

Description

Icon URI

Category

Resource Type siteTemplate

Internal ID gsr7f5e527e_2704_4492_a303_fbf70de71f0d

Content Directory /oracle/webcenter/siteresources/scopedMD/shared

JSPx File /oracle/webcenter/siteresources/scopedMD/s8bb...

Page Definition /oracle/webcenter/siteresources/scopedMD/s8bb...

Metadata File

Created By weblogic

Date Created 12/15/10 2:07 AM

Modified By weblogic

Date Modified 12/15/10 2:07 AM

Attributes

Name	Value

Add More

OK Cancel

See Also: The next thing you do depends on what you want to accomplish. For more information, see:

- [Section 36.5.5.2, "Renaming, Describing, and Categorizing a Resource"](#)
- [Section 36.5.5.3, "Associating an Icon with a Resource"](#)
- [Section 36.5.5.4, "Working with Attributes of a Resource"](#)

36.5.5.2 Renaming, Describing, and Categorizing a Resource

Resources are sorted on the Resource page according to their display names. To maintain a well-organized set of resources, consider developing a standard naming scheme and method of description. This is not a required step, but it may be useful in identifying and clarifying your intended purpose for a given resource.

You can classify your resources into relevant groups. For example, all page styles associated with Sales could be categories under a *sales* category. This value is available and exposed only in the Edit Properties dialog.

To provide a name, description, and category for a resource:

1. Follow the steps outlined in [Section 36.5.5.1, "Accessing the Edit Properties Dialog of a Resource."](#)
2. In the **Display Name** field, edit the display name of the resource, if required.
3. Optionally, in the **Description** field, enter a description of the resource.
4. Optionally, in the **Category** field, enter a category name.
5. Click **OK** to save your changes and exit the dialog.

36.5.5.3 Associating an Icon with a Resource

You can associate an icon with a resource. In the current version of Oracle WebCenter Portal, the associated icon is visible only for page styles when you create a page using the Create Page dialog.

To associate an icon with a resource:

1. Open the Edit Properties dialog as described in [Section 36.5.5.1, "Accessing the Edit Properties Dialog of a Resource."](#)
2. In the **Icon URI** field, enter a standard URI path to the desired icon.

For example, enter:

```
/mycompany/webcenter/page/images/myimage.png
```

You can either specify an absolute URL (where the URL should also work if entered in a browser address field), or a relative URL that points to an image located in the `/oracle/webcenter/siteresources/scopedMD/shared` folder of your application.

3. Click **OK** to save your changes and exit the dialog.

36.5.5.4 Working with Attributes of a Resource

In addition to the default attributes exposed through the Edit Properties dialog (**Display Name**, **Description**, and the like), you can expose custom attributes for resources. The Edit Properties dialog provides an **Attributes** section for entering attribute name/value pairs ([Figure 36–31](#)).

Figure 36–31 Attributes Section of a Resource

Attributes	
Name	Value
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

For example, you can associate the `editPageAfterCreation` attribute with a page style resource to control whether a newly created page opens in edit or view mode. The attribute takes a value of `true` or `false`. When you associate this attribute with a particular page style, every time a user creates a page based on the selected style, the attribute value is considered and the page functions accordingly.

This section describes how to associate a custom attribute with a resource and how to remove a custom attribute. It contains the following sections:

- [Section 36.5.5.4.1, "Associating an Attribute with a Resource"](#)
- [Section 36.5.5.4.2, "Deleting an Attribute of a Resource"](#)

36.5.5.4.1 Associating an Attribute with a Resource To associate an attribute with a resource:

1. Open the Edit Properties dialog using the procedure outlined in [Section 36.5.5.1, "Accessing the Edit Properties Dialog of a Resource."](#)
2. In the **Attributes** section, in the **Name** field, enter the attribute name.
3. In the **Value** field, enter the value of the attribute.

4. Click **Add More** if you want to add more attributes.

This adds a new row. You can then enter the required details in the **Name** and **Value** fields.

5. Click **OK** to save your changes and exit the dialog.

36.5.5.4.2 Deleting an Attribute of a Resource To remove an attribute associated with a resource:

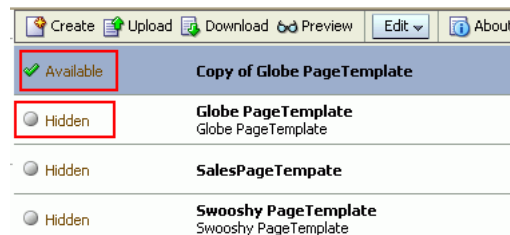
1. Open the Edit Properties dialog using the procedure outlined in [Section 36.5.5.1, "Accessing the Edit Properties Dialog of a Resource."](#)
2. In the **Attributes** section, click the **Remove** icon corresponding to the attribute you want to delete.
3. Click **OK** to save your changes and exit the dialog.

36.5.6 Showing or Hiding a Resource

When you create a resource, by default the resource is marked as hidden. A hidden resource is not available for use in the resource picker. For a resource to become available, it must be published.

For all resources that are available for use, a green tick mark and the word "Available" appear next to the resource's name on the Resources page. A gray icon and the word "Hidden" next to a resource's name indicate that the resource is marked as hidden, as shown in [Figure 36–32](#).

Figure 36–32 Showing or Hiding a Resource



To show or hide a resource:

1. Navigate to the **Resources** page in WebCenter Portal Administration Console, as described in [Section 36.2, "Accessing the WebCenter Portal Administration Console."](#)
2. In the left navigation panel, select the desired type of resource.
3. From the list of resources, select the resource that you want to show or hide.
4. From the **Edit** menu, choose **Show** or **Hide**, depending on the option displayed.

If your resource is hidden, the **Show** option displays on the **Edit** menu. When you click **Show**, a green tick mark and the word "Available" appear next the resource's name, indicating that the resource is now available for use.

If your resource is already published, the **Edit** menu lists the **Hide** option. When you click **Hide**, a gray icon and the word "Hidden" appear next to the resource's name, indicating that the resource is now hidden and is not available to users.

Note: To mark a page as available, select the **Show Page** checkbox next to the page's name on the **Resources** page. If this checkbox is unchecked, the page is marked as hidden.

36.5.7 Setting Resource Security

You can control whether all users or only specific users or groups can access the resources that you created in the application. By default, resource access is controlled by application-level permissions. The Security Settings dialog provides a means of setting aside application-level permissions and defining specific permissions on a selected resource.

For information about setting page access, see [Section 36.5.1.3, "Setting Page Access."](#)

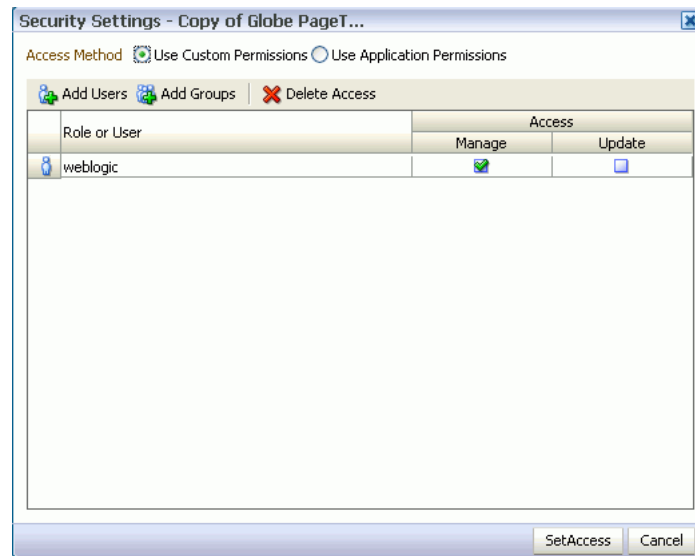
To set access permissions on any resource other than a page:

1. Navigate to the **Resources** page in WebCenter Portal Administration Console, as described in [Section 36.2, "Accessing the WebCenter Portal Administration Console."](#)
2. In the left navigation panel, select the desired type of resource.
3. From the list of resources, select the resource on which you want to set access permissions.
4. From the **Edit** menu, choose **Security Settings**.
5. In the Security Settings dialog, specify an access method by selecting either of the following options ([Figure 36-33](#)):
 - **Use Custom Permissions**—Select this option to define who may manage and update the selected resource. If you select this option, the other controls in the dialog become available. Proceed to step 6.

Note: When you choose **Use Custom Permissions**, ensure that at least one user or group is granted the **Manage** access.

- **Use Application Permissions**—Select this option to inherit the selected resource's access settings from those defined for the application. If you select this option, click **OK** to save your changes and exit the dialog.

Note: Selecting **Use Application Permissions** removes custom permissions that you may have set.

Figure 36–33 Setting Security on a Resource

6. If you selected **Use Custom Permissions**, specify the user or group to whom you want to grant resource access. In the Security Settings dialog:
 - Click **Add Users** to open a dialog where you can search for and select individual users included in your identity store. Select the required user(s), and click **OK** to close the dialog.
 - Click **Add Groups** to open a dialog that you can use to search for and select groups of users included in your identity store. Select the required group(s), and click **OK** to close the dialog.
7. For each user or group listed in the **Role or User** column, specify the level of access you want to grant:
 - Select the **Manage** checkbox to grant full access to the resource. Such users can edit the resource properties and delete the resource.
 - Select the **Update** checkbox to grant the permission to edit the resource. Such users can edit the resource, but cannot delete it.
8. If you want to revoke permissions from any user or group, select that entity and click **Delete Access**.
9. Click **OK**.

36.5.8 Downloading and Uploading a Resource

In your deployed application, you can edit resources at runtime. However, for greater control, you may want to edit a resource at design time. For this, you can download the resource created at runtime, edit it at design time in JDeveloper, and then upload the updated resource back into the application without redeploying the application.

Note: Data controls and pages cannot be downloaded or uploaded at the resource level.

The Download and Upload options enable post-deployment, round-trip application development. These actions greatly simplify the process of bringing new or revised

resources from JDeveloper into your application and pushing them back into development from your application to JDeveloper as needed.

When you download a resource, the resource configuration is saved into a single export archive (.ear file). You can save an export archive either to your local file system or a remote server file system.

To download a resource:

1. Navigate to the **Resources** page in WebCenter Portal Administration Console, as described in [Section 36.2, "Accessing the WebCenter Portal Administration Console."](#)
2. In the left navigation panel, select the desired resource type.
3. From the list of resources, select the resource you want to download as an EAR file.
4. Click **Download**.
5. In the Download dialog, in the **Archive File Name** field, enter the name of the export archive file.
6. In the Download dialog, specify the location where you want to save the export archive file. Use either of the following options:
 - **Save to my computer** - Click this if you want to save the export archive file to your local file system. Then, specify the path where you want to save the file.
 - **Save to WebCenter Portal Server** - Click this to save the export archive file to a remote server file system. In the **Path** field, enter the server path.
7. Click **Download** to download the resource.

After editing your resources in JDeveloper, you can upload them into your application at runtime. For the resources to be uploaded, they must be in the export archive (.ear file) format.

To upload a resource at runtime:

1. Navigate to the **Resources** page in WebCenter Portal Administration Console, as described in [Section 36.2, "Accessing the WebCenter Portal Administration Console."](#)
2. In the left navigation panel, select the desired resource type.
3. Click **Upload**.
4. In the Upload dialog, specify the location of the resource archive file. Depending on the location of your EAR file, select either of the following:
 - **Look on my computer:** Select if the archive is located on your local file system. Enter the path to the EAR file or use the **Browse** button.
 - **Look on WebCenter Portal Server:** Select if the archive is located on a remote server. In the **Path** field, enter the path to the EAR file.
5. Click **Upload**.

36.5.9 Previewing a Resource

You can edit resources at runtime, preview the changes, and make further adjustments as needed.

To preview a resource:

1. Navigate to the **Resources** page in WebCenter Portal Administration Console, as described in [Section 36.2, "Accessing the WebCenter Portal Administration Console."](#)
2. In the left navigation panel, select the desired resource category.
3. Select the resource that you want to preview.
4. Click **Preview**.

Note: Preview of data controls and pages is not supported. The way you access the Preview option differs for certain resources. For information about a particular resource, refer to the resource-specific chapter listed in the table "Resources Available in Spaces" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

36.5.10 Deleting a Resource

When a resource is no longer required, you may want to remove it from your application.

To delete a resource:

1. Navigate to the **Resources** page in WebCenter Portal Administration Console, as described in [Section 36.2, "Accessing the WebCenter Portal Administration Console."](#)
2. In the left navigation panel, select the desired resource type.
3. From the list of resources, select the resource you want to delete.
4. From the **Edit** menu, choose **Delete**.

Note: To delete a page, select the **Delete Page** option from the **Actions** menu of the page. When you delete a page, its sub pages also get deleted.

5. In the Delete confirmation dialog, click **OK** to delete the resource.

36.6 Managing Services, Portlet Producers, and External Applications

You can manage and configure several WebCenter Portal services through the WebCenter Portal Administration Console. From the Services tab ([Figure 36-34](#)), you can manage and configure the content repository, polls, portlet producers, and external applications.

Figure 36–34 WebCenter Portal Administration Console - Services Tab



Some services, such as Analytics, are ready to use out-of-the-box and do not require administrator-level configuration. Other services, such as Polls, require additional configuration by users with administrative privileges to get things up and running.

This chapter includes the following sections:

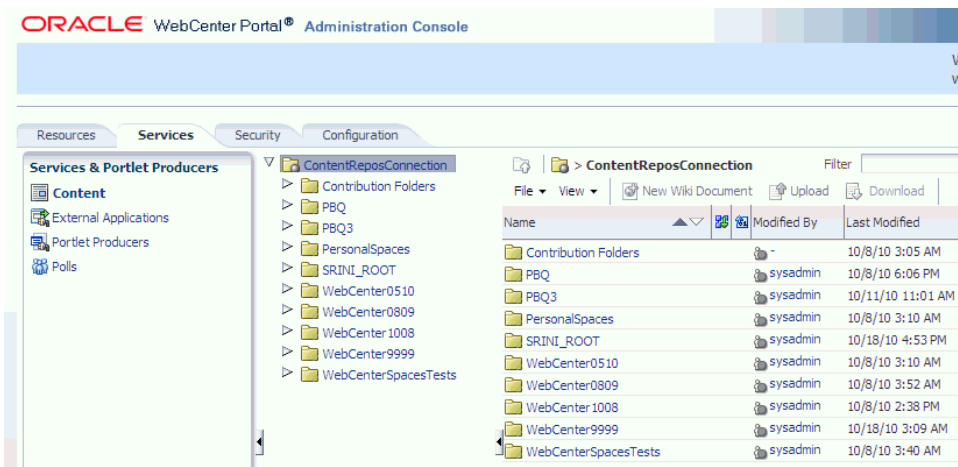
- [Section 36.6.1, "Managing Content"](#)
- [Section 36.6.2, "Managing Portlet Producers"](#)
- [Section 36.6.3, "Managing External Applications"](#)
- [Section 36.6.4, "Creating and Configuring Polls"](#)

36.6.1 Managing Content

Application administrators can manage content that is stored in the application's primary content repository through the WebCenter Portal Administration Console (Figure 36–35). Administrators can add, edit and update content from here, manage document version history, and also access useful information such as direct URLs and download URLs for files and folders.

Your systems administrator is responsible for registering content repositories for Framework applications and determining the primary (or default) content repository. If you expected this administration page to display content from a different content repository, ask your systems administrator to reconfigure the primary (or default) content repository connection. See also, [Section 11.7, "Changing the Active \(or Default\) Content Repository Connection."](#)

Figure 36–35 Contents of a Primary Repository for the Documents Service



This section includes the following subsections:

- [Section 36.6.1.1, "Creating a New Folder"](#)
- [Section 36.6.1.2, "Creating a Wiki Page"](#)
- [Section 36.6.1.3, "Editing a File"](#)
- [Section 36.6.1.4, "Uploading a Document"](#)
- [Section 36.6.1.5, "Checking Out a Document"](#)
- [Section 36.6.1.6, "Uploading a New Version of a Document"](#)
- [Section 36.6.1.7, "Viewing Version History of a Content Item"](#)
- [Section 36.6.1.8, "Getting Direct and Download URLs of a Document"](#)
- [Section 36.6.1.9, "Organizing Columns for the Displayed Content"](#)
- [Section 36.6.1.10, "Setting Up Security on Folders and Documents"](#)

36.6.1.1 Creating a New Folder

To create a new folder:

1. Navigate to the **Services** administration tab.
See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console"](#).
2. Select **Contents**.
3. Select a directory in which you want to create a new folder.
4. From the File menu, choose **New Folder**.
5. In the Create Folder dialog, enter a descriptive name in the **Folder Name** field, and click **Create** to create the folder in the chosen directory.

Tip: To rename or delete a folder, choose the appropriate option from the File menu. This menu also provides options to cut, copy, and paste contents in a folder.

To hide folders in a directory, from the View menu, choose **Hide Folders**. To make hidden folders visible, deselect the **Hide Folders** option.

36.6.1.2 Creating a Wiki Page

To create a wiki document:

1. Navigate to the **Services** administration tab.
See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console"](#).
2. Select **Contents**.
3. Select a directory in which you want to create your wiki page.
4. Click **New Wiki Document**. The Rich Text Editor displays.
5. In the **Title** field, enter a descriptive title, and click **Create** to create the wiki page in the chosen directory.

36.6.1.3 Editing a File

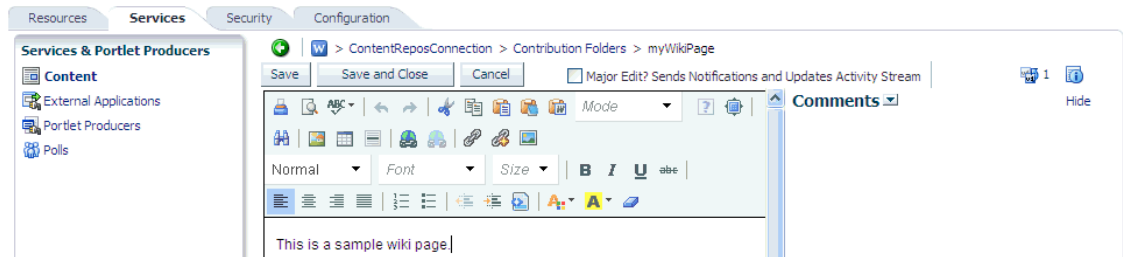
To edit contents such as a wiki document:

1. Navigate to the **Services** administration tab.

See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console"](#).

2. Select **Contents**.
3. Select the item you want to edit.
4. From the File menu, choose **Edit**. The file opens in the Rich Text Editor, as shown in [Figure 36–36](#).

Figure 36–36 A Wiki Page Opened for Editing



5. Click **Save and Close** to close the document after saving.

36.6.1.4 Uploading a Document

To upload a document:

1. Navigate to the **Services** administration tab.
See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console"](#).
2. Select **Contents**.
3. Select a directory in which you want to upload your document.
4. Click **Upload Document**. The Upload Document to <Folder Name> dialog displays.
5. In the **Upload Document** section, click **Browse** and select the required document. In the **Description** section you can enter a description if you like, and then click **Upload**. Your document is uploaded in the chosen directory.

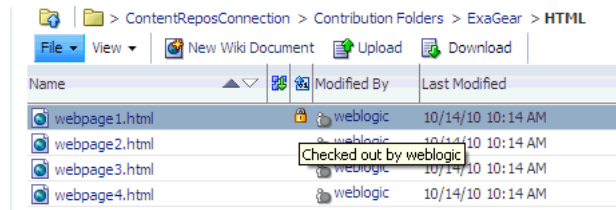
Tip: You can upload multiple documents at a time. You can add more field to upload as many documents as you like by clicking **More**.

To download a document, select it and click **Download**.

36.6.1.5 Checking Out a Document

To check out a document:

1. Navigate to the **Services** administration tab.
See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console"](#).
2. Select **Contents**.
3. Select the document you want to check out.
4. From the File menu, choose **Check Out**. The document is checked out and the lock icon appears to indicate its checked out status, as shown in [Figure 36–37](#).

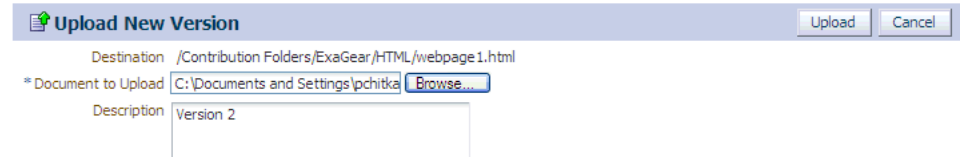
Figure 36–37 Checked Out Document

Tip: To cancel check out, select the document in the directory it is located, and from the File menu choose **Cancel Check Out**.

36.6.1.6 Uploading a New Version of a Document

To upload a new version of a document:

1. Navigate to the **Services** administration tab.
See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console"](#).
2. Select **Contents**.
3. Select the document you want to check out.
4. From the File menu, choose **Upload New Version**.
5. In the Upload New Version dialog, click **Browse** to select another version of the document, as shown in [Figure 36–38](#). You can enter a description, if you like, and then click **Upload**.

Figure 36–38 Upload a New Version of a Document

36.6.1.7 Viewing Version History of a Content Item

To view the version history of a document such an image or a wiki page:

1. Navigate to the **Services** administration tab.
See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console"](#).
2. Select **Contents**.
3. Navigate to the directory in which your documents are located.
4. Select a document to view its version history.
5. From the View menu, choose **Version History**. The version history displays, as shown in [Figure 36–39](#).

Figure 36–39 Version History of a Document



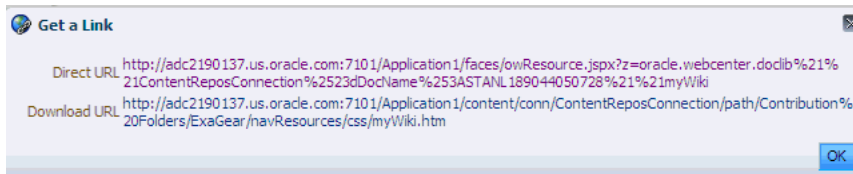
Tip: To view properties of an item, select this item in the directory it is located, and from the View menu, choose **Properties**.

36.6.1.8 Getting Direct and Download URLs of a Document

A direct URL lets you view a document, whereas a download URL lets you download it. To get these URLs:

1. Navigate to the **Services** administration tab.
See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console"](#).
2. Select **Contents**.
3. Navigate to the directory in which your documents are located.
4. Select a document to get its URLs.
5. From the View menu, choose **Get a Link**.
6. In the Get a Link dialog, click the **Direct URL** if you want to view this document. To download this document, click **Download URL**.

Figure 36–40 Direct and Download URLs

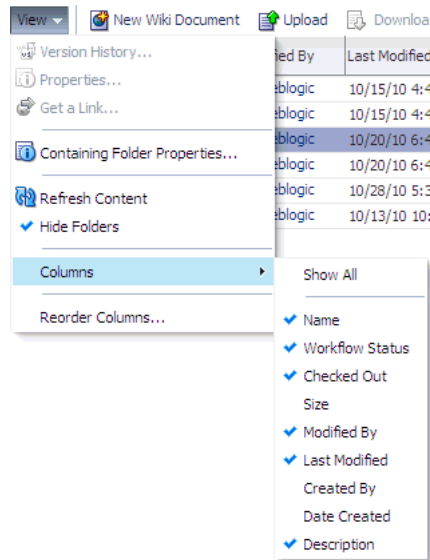


36.6.1.9 Organizing Columns for the Displayed Content

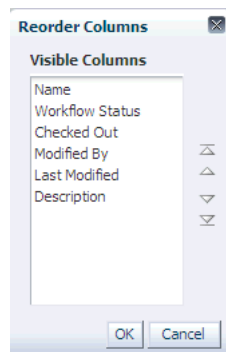
For each item in a primary repository you can choose what associated information you would like to display, such as name of a content item, its last modified date, its check out status, and so on. You can also reorder chosen columns to display the desired information in a specific order.

36.6.1.9.1 Showing Columns To choose columns that will display the desired information associated with your content items:

1. Navigate to the **Services** administration tab.
See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console"](#).
2. Select **Contents**.
3. Navigate to the directory in which your documents are located.
4. From the View menu, choose **Columns** and then choose titles that will display the desired information for your content items, as shown in [Figure 36–9](#).

Figure 36–41 Columns - Show**36.6.1.9.2 Reordering Columns** To reorder columns:

1. Navigate to the **Services** administration tab.
See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console"](#).
2. Select **Contents**.
3. Navigate to the directory in which your documents are located.
4. From the View menu, choose **Reorder Columns**. The Reorder Columns dialog displays, as shown in [Figure 36–42](#).

Figure 36–42 Columns - Reorder**36.6.1.10 Setting Up Security on Folders and Documents**

Under the Contents tab, in the File menu, the Security menu item for a document or folder is visible when the following conditions are met:

- Item level security has been enabled in Oracle WebCenter Content Server, as described in [Section 11.2.3.10, "Configuring Item Level Security in WebCenter Portal Applications."](#)
- If the security group assigned to these documents is listed in the SpecialAuthGroups setting at the time when the item level security is enabled

in Oracle WebCenter Content Server, as described in [Section 11.2.3.10, "Configuring Item Level Security in WebCenter Portal Applications."](#)

- The user has administrative rights on the document or folder in Oracle WebCenter Content Server.

For information about using the security feature, see the section "Setting Security Options for a File" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

36.6.2 Managing Portlet Producers

To be able to register and manage portlet producers in a Framework application, a user must be assigned the `AppConnectionManager` role. By default, users with the `Administrator` role have the `AppConnectionManager` role; and therefore, application administrators can configure portlet producers through the WebCenter Portal Administration Console. See also, [Section 36.4.4, "Managing Application Roles and Permissions"](#).

When you register a portlet producer, all the portlets owned by that producer automatically become available through the application's resource catalog. Once registered, users with appropriate edit page privileges, are then able to add the producer's portlets to their pages. Users who want access to a particular portlet but cannot find it in the resource catalog must ask an administrator to register the associated producer.

This section includes the following:

- [Section 36.6.2.1, "Registering Portlet Producers"](#)
- [Section 36.6.2.2, "Editing and Deleting Portlet Producers"](#)

Note: Fusion Middleware administrators can also register portlet producers for Framework applications, using Fusion Middleware Control and WLST commands. For details, see [Chapter 24, "Managing Portlet Producers."](#)

36.6.2.1 Registering Portlet Producers

To register a portlet producer at runtime for a Framework application:

1. Navigate to the **Services** administration tab.

See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console"](#).

2. Select **Portlet Producers** ([Figure 36–43](#)).

Figure 36–43 WebCenter Portal Administration Console - Portlet Producers

3. Click **Register**.
4. Enter connection details for the portlet producer.

If you need help with one or more fields, refer to the following tables:

WSRP Producers

- [Table 24–1, "WSRP Producer Connection Parameters"](#)
- [Table 24–2, "WSRP Producer Security Connection Parameters"](#)
- [Table 24–3, "WSRP Producer Key Store Connection Parameters"](#)

Oracle PDK Java Producers

- [Table 24–4, "Oracle PDK-Java Producer Connection Parameters"](#)

Pagelet Producers

- [Table 25–1, "Pagelet Producer Connection Parameters"](#)

5. Click **Test** to verify your connection details.
6. Click **OK** to register the portlet producer.

36.6.2.2 Editing and Deleting Portlet Producers

To modify or delete portlet producers at runtime for a Framework application:

1. Navigate to the **Services** administration tab.
See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console"](#).
2. Select **Portlet Producers** (Figure 36–43).
3. Select the portlet producer required, and then click one of the following:
 - Click **Edit** to update connection details for a portlet producer.
 - Click **Deregister** to deregister a producer. This removes registration data from both the Framework application and the remote producer.

Deregistering *does not* remove portlet instance from Framework application pages. Instead of the portlet, users see a "Portlet unavailable" message.

Consider deleting the external application associated with this portlet producer if the application's sole purpose is to support this producer. See [Section 36.6.3.2, "Editing and Deleting External Applications."](#)

36.6.3 Managing External Applications

To be able to register and manage external applications in a Framework application, a user must be assigned the `AppConnectionManager` role. By default, users with the

Administrator role have the `AppConnectionManager` role; and therefore, application administrators can configure external applications through the WebCenter Portal Administration Console. See also, [Section 36.4.4, "Managing Application Roles and Permissions"](#).

An external application is any application that implements its own authentication process. Specifically, it is an application that does not take part in the Framework application's single sign-on process. If your Framework application interacts with an application that handles its own authentication, you can register an external application to allow for credential provisioning.

Application administrators can register, edit, and delete external applications for a Framework application at runtime, through the WebCenter Portal Administration Console.

This section includes the following subsections:

- [Section 36.6.3.1, "Registering External Applications"](#)
- [Section 36.6.3.2, "Editing and Deleting External Applications"](#)

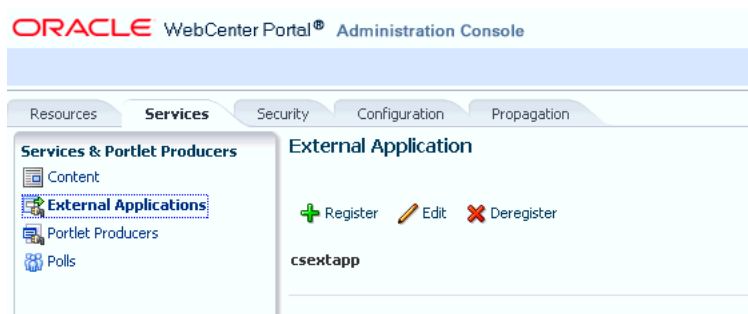
Note: Fusion Middleware administrators can also register external applications for Framework applications, using Fusion Middleware Control and WLST commands. For details, see [Chapter 24, "Managing Portlet Producers."](#)

36.6.3.1 Registering External Applications

To register an external application at runtime for a Framework application:

1. Navigate to the **Services** administration tab.
See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console"](#).
2. Select **External Application** (Figure 36–44).

Figure 36–44 WebCenter Portal Administration Console - External Applications



3. Click **Register**.
4. Enter connection details for the external application.

If you need help with one or more fields, refer to the following tables:

- [Table 26–1, "External Application Connection - Name"](#)
- [Table 26–2, "External Application Connection - Login Details"](#)
- [Table 26–3, "External Application Connection - Authentication Details"](#)
- [Table 26–4, "External Application Connection - Additional Login Fields"](#)

- [Table 26–5, "External Application Connection - Shared User and Public User Credentials"](#)
5. Click **Test** to verify your connection details.
 6. Click **OK** to register the application.

36.6.3.2 Editing and Deleting External Applications

To modify or delete external applications at runtime for a Framework application:

1. Navigate to the **Services** administration tab.
See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console"](#).
2. Select **External Application** ([Figure 36–44](#)).
3. Select the external application required and then click one of the following:
 - Click **Edit** to update connection details for an external application.
 - Click **Deregister** to remove the external application.

Take care when deleting an external application connection as Framework application users will no longer have access to that application, and any services dependent on the external application may not function correctly.

36.6.4 Creating and Configuring Polls

Application administrators can create and configure online polls for a Framework application at runtime through the WebCenter Portal Administration Console. With polls, you can survey your audience (such as their opinions and their experience level), check whether they can recall important information, and gather feedback on the efficacy of presentations.

This section includes the following subsections:

- [Section 36.6.4.1, "What You Should Know About the Polls Service"](#)
- [Section 36.6.4.2, "Creating, Configuring, and Analyzing a Poll"](#)

36.6.4.1 What You Should Know About the Polls Service

With the Polls service, in addition to taking available polls, you can do the following:

- Create a poll by clicking the **Create Poll** icon, and then adding section headings and questions to it
- Schedule the poll for distribution
- Save the poll as a template for use with new polls
- Analyze the results of the poll

The Polls service is integrated with many WebCenter Portal services, such as RSS, Search (to search poll text), Instant Messaging and Presence, and Recent Activities.

[Figure 36–45](#) shows an example poll.

Figure 36–45 Example Poll

Polls must be published and open before they can be completed by users. Users cannot complete unpublished or closed polls.

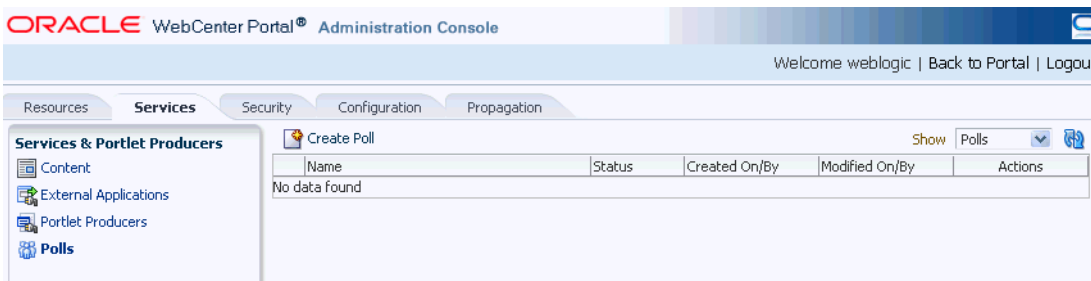
36.6.4.2 Creating, Configuring, and Analyzing a Poll

From the Polls page (Figure 36–46) you can create polls, and once created, view the status of current polls and perform operations on them, including edit, save (as poll or as a poll template), publish, close, analyze, and delete. You can update poll data on the Polls page at any time by clicking the **Refresh** icon.

To add a new poll:

1. Navigate to the **Services** administration tab.
See also, [Section 36.2, "Accessing the WebCenter Portal Administration Console"](#).
2. Select **Polls** (Figure 36–46).

Figure 36–46 WebCenter Portal Administration Console - Polls



3. Click **Create Poll**.

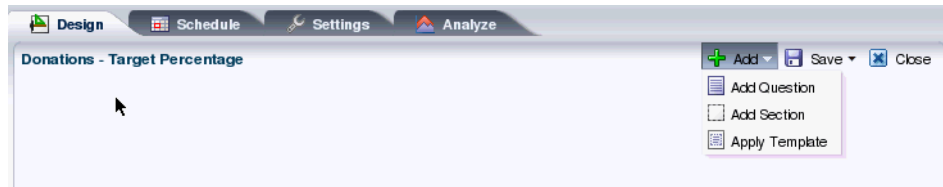
The Create Poll dialog displays (Figure 36–47).

Figure 36–47 Create Poll Dialog

4. Enter a Name and Description for the poll and click **Create**.

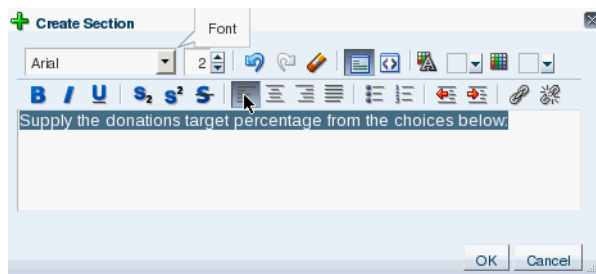
The Design tab displays (Figure 36–48).

Figure 36–48 Create Polls - Design Tab



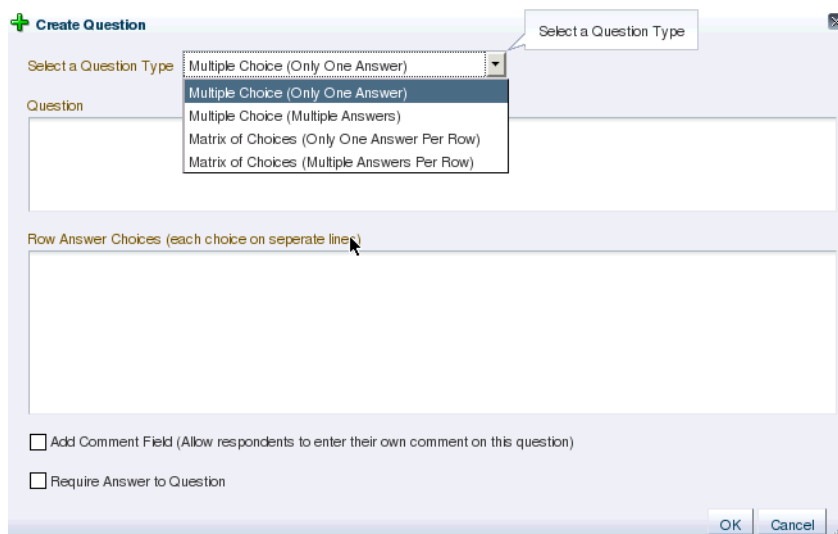
5. Click **Add** to populate the poll with an existing template, or with questions and surrounding text.
6. Click **Add Section** to enter any explanatory text in a rich text editor (Figure 36–49), and click **OK** when done.

Figure 36–49 Polls - Create/Edit Section Dialog



7. Click **Add Question** to add each poll question (Figure 36–50).

Figure 36–50 Polls - Create/Edit Question Dialog - Question Type



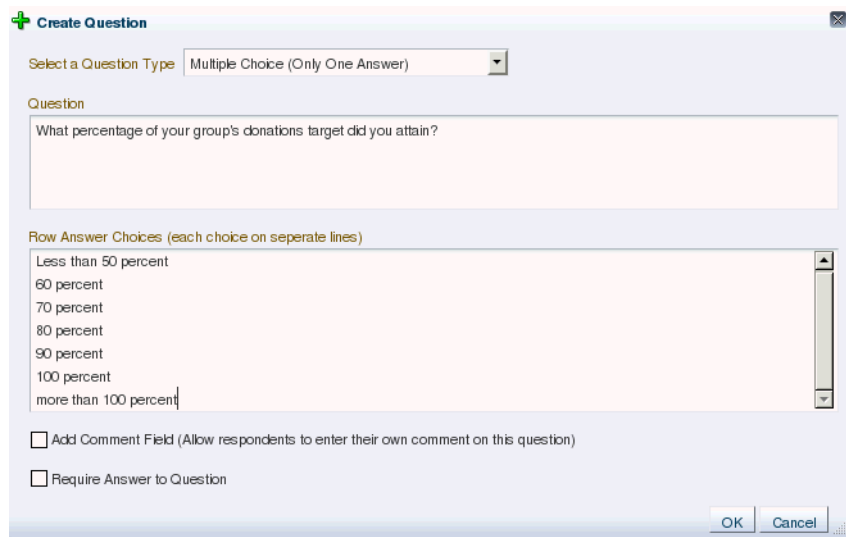
8. Select the Question Type from the dropdown list.

There are four question types:

- Multiple Choice (Only One Answer)

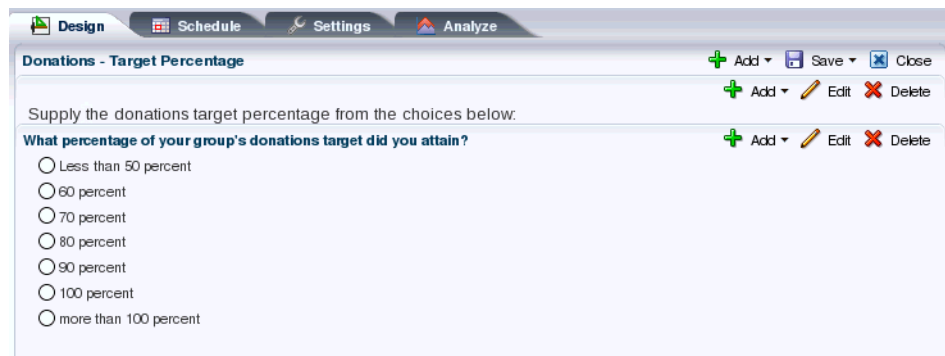
- Multiple Choice (Multiple Answer)
 - Matrix of Choices (Only One Answer Per Row)
 - Matrix of Choices (Multiple Answers Per Row)
9. Enter the Question text and the Choices (each choice must be on a separate line) and click **OK** when done.

Figure 36–51 Polls - Create/Edit Question Dialog



For this example, the current design looks like [Figure 36–52](#).

Figure 36–52 Create Polls - Design Tab



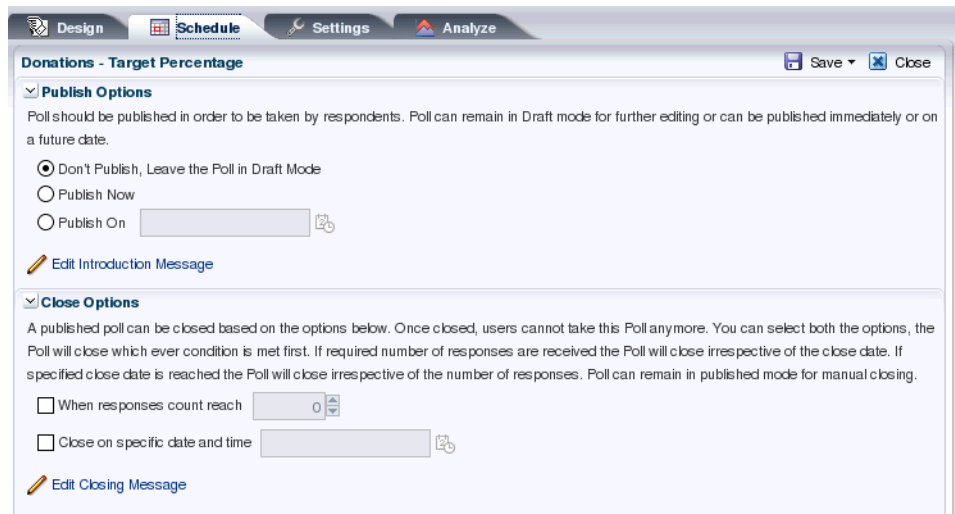
10. Open the **Schedule** tab, and choose the publish and close options for the poll (see [Figure 36–53](#)). Polls must be published and open to be taken. Users cannot take unpublished or closed polls.

In Publish Options, choose to keep the poll in draft mode for further editing, publish it immediately, or publish it on a future date. Click the **Select Date and Time** icon to enter the publishing time through a calendar. Click **Edit Introduction Message** to customize in the rich text editor the text provided at the beginning of the poll.

In Close Options, choose to close the published poll after it reaches a certain number of responses or on a certain date. If you choose both options, then the poll closes when either condition is first met. Click the **Select Date and Time** icon to

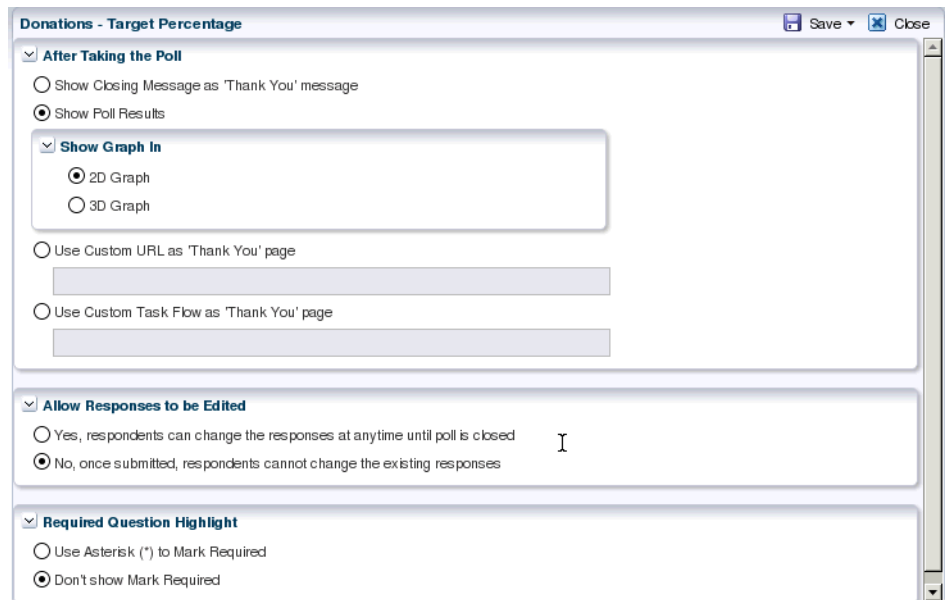
enter the closing time through a calendar. Click **Edit Closing Message** to customize in the rich text editor the text provided at the end of the poll.

Figure 36–53 Create Polls - Schedule Tab



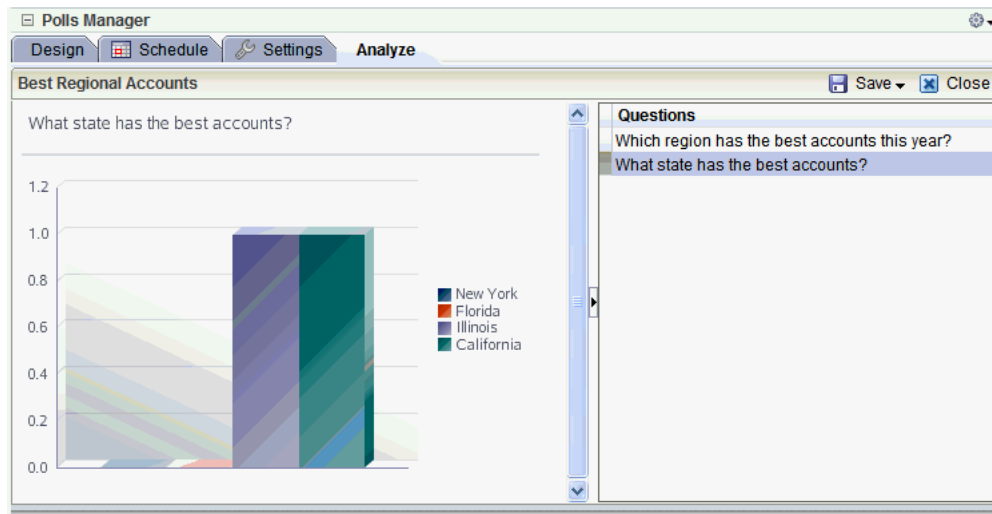
11. Open the **Settings** tab and choose what to display after the poll is taken, if users can edit responses after entering them, and if an asterisk should mark required questions (see [Figure 36–54](#)).

Figure 36–54 Create Polls - Settings Tab



12. After conducting the poll, open the **Analyze** tab to view the poll data. Use the Questions box on the right to toggle between multiple questions ([Figure 36–55](#)).

Figure 36–55 Create Polls - Analyze Tab



Managing a Multilanguage Portal

If your portal must support different languages, you can configure it to display localized content based on the user's selected language and locale. For example, if you know your page will be viewed by users who speak Italian, you can localize your page so that when Italian is selected (in browser, user preferences, space, or application settings), text strings in the page appear in Italian.

Additionally, locale selection applies special formatting considerations applicable to the selected locale. For example, whether information is typically viewed from left to right or right to left, how numbers are depicted (such as monetary information), and the like.

This chapter includes the following sections:

- [Section 37.1, "What You Should Know About Languages in the Spaces Application"](#)
- [Section 37.2, "Limiting Edits to a Particular String or Space"](#)
- [Section 37.3, "Modifying Strings"](#)
- [Section 37.4, "Adding Support to Spaces for a New Language"](#)
- [Section 37.5, "Presenting Translated Content Through a Content Presenter Template"](#)

For information on language configuration options available in Spaces, see *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

37.1 What You Should Know About Languages in the Spaces Application

There are three main types of information that are displayed in the Spaces application:

- User interface (UI) elements, such as field and button labels and seeded boilerplate text
- User-entered metadata, such as page names, the space name, and the space description
- Content added by users, such as announcements, documents, and discussion forum content

Each type of information is handled differently when it comes to modification:

- UI elements:

Note: UI elements include out-of-the-box translations for 27 languages and 100 different locales. You need only change this text if the default UI text is not suited to your company’s needs or if your company must support additional languages.

- To change the text for your entire site (rather than just one space), edit the strings in the override bundle.
- To change the UI text for a particular space, edit the strings in the space-specific resource bundle.
- User-entered metadata (such as page names, the space name, and the space description) is saved as strings in the resource bundle for the space. Each space has its own resource bundle. To change the user-entered metadata, edit the strings in this space-specific resource bundle.

Note: Generally, the user-entered metadata you want to display in multiple languages is company-wide content or customer-facing content that likely has translations available in some form. More specific content (for example, content specific to a particular department or region) is probably necessary in only one language, and therefore does not require translation.

- Content added by users is generally displayed in the language used by the contributing user, though there is a way that you can display translated content using Content Presenter.

37.1.1 Languages Supported Out-of-the-Box by Spaces

Spaces provides run-time translations for 27 languages and 100 different locales.

Table 37–1 Languages Available in Spaces

A to Fi	Fr to No	P to T
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

The list in [Table 37–1](#) includes all the languages available to Spaces out-of-the-box. Users can also select locales associated with particular languages. For example, a user can change the language to Arabic and, within that language group, select from 20 different locales, including Algeria, Bahrain, Djibouti, and so on.

Note: The administrative tier that offers services to Spaces, including such tools as Oracle Enterprise Manager, provides a subset of the languages available to Spaces. These include:

- English
- Brazilian Portuguese
- Chinese (Simplified)
- Chinese (Traditional)
- French
- German
- Italian
- Japanese
- Korean
- Spanish

The Discussions service uses WebCenter Portal's Discussion Server. Out-of-the-box, the discussion server application supports English and Spanish. It does not support other languages listed in [Table 37-1](#). However, the application is open to your own translation files. For more information, see

<http://www.jivesoftware.com/builds/docs/latest/documentation/developer-guide.html#i18n>. This information is explicit to the discussion server application user interface.

37.2 Limiting Edits to a Particular String or Space

You might need only to edit a particular string or the strings for a particular space. In that case, you need to find the values associated with the string or the space:

- [Section 37.2.1, "Finding the Resource Key for a String"](#)
- [Section 37.2.2, "Finding the GUID for a Space"](#)

37.2.1 Finding the Resource Key for a String

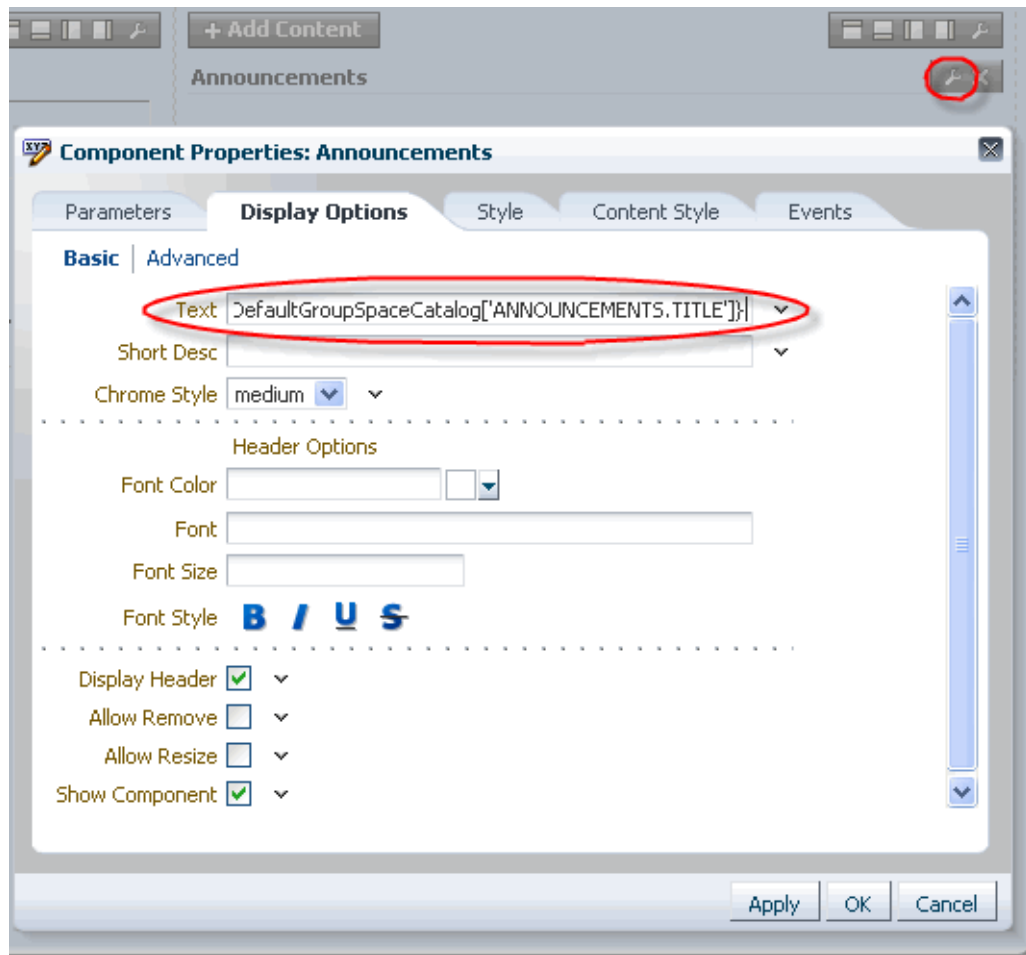
If you want to edit a particular string, you need to know the resource key for the string so you can find it in the string files.

To find the resource key for a string:

1. Open the page or resource in Composer. For details, see "Editing a Page Template in Composer", "Editing a Page in a Space" or "Editing a Task Flow" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.
2. Click the **Edit** icon (wrench) for the component that includes the string you want to edit.
3. In the Component Properties dialog box, click the **Display Options** tab.
4. The resource key is the last part of the text in the **Text** box.

For example, [Figure 37-1](#) shows the resource key for the Announcements component. If you want to edit the string "Announcements" make note of the resource key `ANNOUNCEMENTS.TITLE`.

Figure 37-1 Display Options for Announcements Component - Resource Key



37.2.2 Finding the GUID for a Space

If you want to edit the UI text for a particular space or edit user-entered metadata, you need to find the GUID for the space.

To find the GUID for a space:

1. Navigate to the space that includes the strings you want to edit.
2. Click the **Actions** menu, choose **About**, then choose **This Space**.
3. In the This Space dialog box, note the **Internal ID** value.

Figure 37-2 GUID for a Space



37.3 Modifying Strings

Whether you are modifying UI text site-wide, UI text for a particular space, or user-entered metadata in a space, the process is basically the same, you just modify different files. To modify UI text site-wide, you edit the override bundle (SpacesSeedDataOverrideBundle.xlf). To modify UI text or user-entered metadata for a particular space, you edit the space-specific resource bundle (scope-resource-bundle.xlf).

To modify strings:

1. Use the WLST command `exportMetadata` to export the string files:
 - To export all strings, do not include the `docs` attribute. For example:

```
exportMetadata(application='webcenter', server='WC_Spaces', toLocation='/tmp/metadata')
```

This example exports all string files from the “webcenter” application on the “WC_Spaces” server to the “/tmp/metadata” folder. Always use “webcenter” as the application name. Change server name to match the server that hosts your installation of Spaces. Change the `toLocation` to the location into which you want to export the string files.

- To export only specific string files, include the `docs` attribute. For example:

```
exportMetadata(application='webcenter', server='WC_Spaces', toLocation='/tmp/metadata', docs='/xliifBundles/SpacesSeedDataOverrideBundle.xlf,/oracle/webcenter/translations/scopedMD/SPACE_GUID/scope-resource-bundle.xlf')
```

This example produces similar results to the first example, but exports only the site-wide override bundle and a space-specific resource bundle.

- To edit site-wide UI strings, use the first `docs` value that points to the `SpacesSeedDataOverrideBundle.xlf`.
- To edit space-specific UI strings and user-entered metadata, use the second `docs` value that points to the `scope-resource-bundle.xlf`, replacing `SPACE_GUID` with the GUID of the space for which you are modifying strings.

Note: To export more than one file, separate file locations with commas.

For more information, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#) See also "exportMetadata" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

2. Navigate to the folder into which you exported the string files, and open the string file in a text editor.

Caution: Make sure to correctly encode your edited file or you receive an error when you try to import the translations. We recommend using Oracle JDeveloper to edit the file because it automatically encodes special characters correctly.

- To edit the site-wide UI text, open `/xliffBundles/SpacesSeedDataOverrideBundle.xlf`.
 - To edit space-specific UI text or user-entered metadata, open `/oracle/webcenter/translations/scopedMD/SPACE_GUID/scope-resource-bundle.xlf`, replacing `SPACE_GUID` with the GUID of the space for which you are modifying strings.
3. Find the `<trans-unit>` blocks you want to modify.

The `ID` attribute (in `SpacesSeedDataOverrideBundle.xlf`) or `OBJECTGUID` attribute (in `scope-resource-bundle.xlf`) corresponds to the resource key you made note of when looking at the component in Composer.

For example, here is the `<trans-unit>` block for the Announcements title in site-wide `SpacesSeedDataOverrideBundle.xlf` file.

```
<trans-unit id="ANNOUNCEMENTS_TITLE">
<source>Announcements</source>
</trans-unit>
```

Here is the `<trans-unit>` block for the Announcements title in a space-specific `scope-resource-bundle.xlf` file.

```
<trans-unit id="SCOPEGUID:s1a448c10_c9b8_429f_bf83_
a481d5f9e4bc:SERVICEID:oracle.webcenter.peopleconn:OBJECTTYPE:profile:OBJECTGUI
D:ANNOUNCEMENTS_TITLE">
<source>Announcements</source>
</trans-unit>
```

4. Edit the text in the `<source>` block to fit your business needs, then save the file.

- Use the WLST command `importMetadata` to import the updated string files back into Spaces. For example:

- To import all strings, do not include the `docs` attribute. For example:

```
importMetadata(application='webcenter',server='WC_Spaces',fromLocation='/tmp/metadata')
```

This example imports all string files from the “/tmp/metadata” folder to the “webcenter” application on the “WC_Spaces” server. Change the `fromLocation` to the location from which you want to import the string files. Always use “webcenter” as the application name. Change server name to match the server that hosts your installation of Spaces.

- To import only specific string files, include the `docs` attribute:

```
importMetadata(application='webcenter',server='WC_Spaces',fromLocation='/tmp/metadata',docs='/xliiffBundles/SpacesSeedDataOverrideBundle.xlf,/oracle/webcenter/translations/scopedMD/SPACE_GUID/scope-resource-bundle.xlf')
```

This example produces similar results to the first example, but imports only the site-wide override bundle and a space-specific resource bundle.

- To import site-wide UI strings, use the first `docs` value that points to the `SpacesSeedDataOverrideBundle.xlf`.
- To import space-specific UI strings and user-entered metadata, use the second `docs` value that points to the `scope-resource-bundle.xlf`, replacing `SPACE_GUID` with the GUID of the space for which you are modifying strings.

Note: To import more than one file, separate file locations with commas.

For details, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#) See also "importMetadata" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

- Restart the WC_Spaces managed server, and confirm that the changes you made appear in the UI.

37.4 Adding Support to Spaces for a New Language

If you want to support a language in Spaces that is not supported out-of-the-box provide string files for the new language, and add a `<language>` tag for the new language in the `supported-languages.xml` configuration file.

To add support for a new language:

- Use the WLST command `exportMetadata` to export the string files. For example:

```
exportMetadata(application='webcenter',server='WC_Spaces',toLocation='/tmp/metadata')
```

This example exports all string files for a Spaces application (“webcenter”) deployed on the “WC_Spaces” server to the “/tmp/metadata” folder. If necessary, change the server name to match your Spaces installation. You must

change the `toLocation` to the location into which you want to export the string files.

For more information, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#) See also "exportMetadata" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

2. Create a language/locale-specific version of each string file you want to translate. For example, to translate the site-wide UI text into Catalina, create `SpacesSeedDataOverrideBundle_ca.xlf`.

- To translate site-wide UI text, copy `/xliffBundles/SpacesSeedDataOverrideBundle.xlf`.
- To translate space-specific UI text or user-entered metadata, copy `/oracle/webcenter/translations/scopedMD/SPACE_GUID/scope-resource-bundle.xlf`, replacing `SPACE_GUID` with the GUID of the space.

Note: There are probably very few spaces that need to support new languages. However, you might want some spaces to be translated into the newly supported language (for example, any company-wide spaces).

3. Translate each language/locale-specific string file:

- a. Open one of the copied string files in a text editor.

Caution: Make sure to correctly encode your edited file or you receive an error when you try to import the translations. We recommend using Oracle JDeveloper to edit the file because it automatically encodes special characters correctly.

- b. Translate the `<source>` text in each `<trans-unit>` block.

Here is an example of a `<trans-unit>` block from the site-wide `SpacesSeedDataOverrideBundle.xlf` file.

```
<trans-unit id="ANNOUNCEMENTS_TITLE">
<source>Announcements</source>
</trans-unit>
```

Here is an example of a `<trans-unit>` block from a space-specific `scope-resource-bundle.xlf` file.

```
<trans-unit id="SCOPEGUID:s1a448c10_c9b8_429f_bf83_
a481d5f9e4bc:SERVICEID:oracle.webcenter.peopleconn:OBJECTTYPE:profile:OBJEC
TGUID:ANNOUNCEMENTS_TITLE">
<source>Announcements</source>
</trans-unit>
```

- c. Save the file.
 - d. Repeat these steps for each string file you want to translate.
4. Use the WLST command `importMetadata` to import the updated string files back into Spaces. For example:

```
importMetadata(application='webcenter', server='WC_
```

```
Spaces',fromLocation='/tmp/metadata')
```

This example imports all string files from the “/tmp/metadata” folder to a Spaces application (“webcenter”) deployed on the “WC_Spaces” server. If necessary, change the server name to match your Spaces installation. Change the `fromLocation` to the location from which you want to import the string files.

For details, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#) See also "importMetadata" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

5. Add the new language to the supported-languages.xml file.
 - a. In Oracle JDeveloper, open supported-languages.xml.
 - b. Add a `<language>` tag for the new language. For example, to support Catalina, add the following:

```
<language name="Catalina" id="ca" used="true" translated="true"/>
```

Specify the language name you want to appear in the UI as the value for the `name` attribute.

Specify the language ID you added as the suffix of your translated string files as the value for the `id` attribute.

6. Deploy the updated language list:
 1. Ensure that the CustomLanguageAdditions project is selected in the deployment profile.
 2. Build and deploy the customized Spaces .WAR. For details, see “Extending Spaces Using JDeveloper” in *Oracle Fusion Middleware Developer’s Guide for Oracle WebCenter Portal*.
7. Restart the WC_Spaces managed server, and confirm your changes appear in the user interface.

37.5 Presenting Translated Content Through a Content Presenter Template

To display translated content, you must create a Content Presenter template that looks up the display language and then displays content from a language-specific folder. For information on creating a Content Presenter template, see “Creating Content Presenter Display Templates” in *Oracle Fusion Middleware Developer’s Guide for Oracle WebCenter Portal*.

Monitoring Oracle WebCenter Portal Performance

Fusion Middleware Control Console provides a Web-based user interface for monitoring the real-time performance of WebCenter Portal applications (Framework applications and Spaces applications), including any producers and portlets that WebCenter Portal 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 Portal 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 Portal diagnostic log files.

Administrators who monitor WebCenter Portal applications regularly will learn to recognize trends as they develop and prevent performance problems in the future.

This chapter includes the following sections:

- [Section 38.1, "Understanding Oracle WebCenter Portal Performance Metrics"](#)
- [Section 38.2, "Viewing Performance Information"](#)
- [Section 38.3, "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"](#).

38.1 Understanding Oracle WebCenter Portal Performance Metrics

Through Fusion Middleware Control, administrators can monitor the performance and availability of all the components and services that make up WebCenter Portal applications, and 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 Portal's performance metrics are listed and described here for your reference. Some applications (such as Spaces applications) might use the full range of social networking, personal productivity, and collaboration service metrics listed, while others may only use one or two of these services.

This section includes the following subsections:

- [Section 38.1.1, "WebCenter Portal Metric Collection: Recent History and Since Startup"](#)
- [Section 38.1.2, "Common WebCenter Portal Metrics"](#)
- [Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions"](#)
- [Section 38.1.4, "WebCenter Portal Service-Specific Metrics"](#)
- [Section 38.1.5, "WebCenter Portal Service-Specific Performance Issues and Actions"](#)
- [Section 38.1.6, "Space Metrics"](#)
- [Section 38.1.7, "Page Metrics"](#)

38.1.1 WebCenter Portal Metric Collection: Recent History and Since Startup

Performance metrics are automatically enabled for Oracle WebCenter Portal. 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 metrics are collected for Oracle WebCenter Portal:

- **Since Startup:** At any given time, real-time metrics are available for the duration for which the WebLogic Server hosting WebCenter Portal applications is up and running. Real-time metrics that are collected or aggregated since the startup of the container are displayed for WebCenter Portal as **Since Startup**. These metrics provide data aggregated over the lifetime 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 before the restart becomes unavailable.

- **Recent History:** In addition to the **Since Startup** metrics, Oracle WebCenter Portal metrics are also configured to capture performance data every five minutes. This metric data is used with the Since Startup metrics, and is made available as **Recent History** metrics.
- All metrics seen under Recent History are calculated using 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, while 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 run-time access.

Typically, Recent History shows data for the most recent 10-15 minutes. However, there are situations when the data does not reflect the last 10-15 minutes:

- If the WebLogic Server has just 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. 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 most recent 10-15 minutes.

While diagnosing a live site, you can navigate to the WebCenter Portal 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 a long time. If needed, navigate to application pages that use the service and set the application to trigger the run-time metrics to get more data.

38.1.2 Common WebCenter Portal Metrics

Fusion Middleware Control provides capabilities to monitor performance of WebCenter Portal services in the following ways:

- Services summary: Summary of performance metrics for each service used in a WebCenter Portal application. [Table 38–1](#) lists services that use common performance metrics. [Table 38–2](#) describes service metrics.
- Most popular operations and response time for individual service operations. [Table 38–3](#) describes these metrics.
- Per operation metrics: Performance metrics for individual service operations. [Table 38–1](#) lists common performance metrics used to monitor performance of individual operations. [Table 38–3](#) describes these metrics.

Table 38–1 Common Performance Metrics

Service	Services Summary (Since Startup and Recent History)	Per Operation Metrics (Since Startup and Recent History)
Announcements	The performance metrics include: <ul style="list-style-type: none"> ■ Status ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms) 	The performance metrics include: <ul style="list-style-type: none"> ■ Most Popular Operations ■ Response Time ■ Invocations ■ Average Time (ms) ■ Maximum Time (ms) (Since Startup only)
BPEL Worklist	The performance metrics include: <ul style="list-style-type: none"> ■ Status ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms) 	Not applicable
Discussion Forums	The performance metrics include: <ul style="list-style-type: none"> ■ Status ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms) 	The performance metrics include: <ul style="list-style-type: none"> ■ Most Popular Operations ■ Response Time ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms) ■ Maximum Time (ms) (Since Startup only)

Table 38–1 (Cont.) Common Performance Metrics

Service	Services Summary (Since Startup and Recent History)	Per Operation Metrics (Since Startup and Recent History)
External Applications	The performance metrics include: <ul style="list-style-type: none"> ■ Status ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms) 	The performance metrics include: <ul style="list-style-type: none"> ■ Most Popular Operations ■ Response Time ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms) ■ Maximum Time (ms) (Since Startup only)
Events	The performance metrics include: <ul style="list-style-type: none"> ■ Status ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms) 	The performance metrics include: <ul style="list-style-type: none"> ■ Most Popular Operations ■ Response Time ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms) ■ Maximum Time (ms) (Since Startup only)
Import/Export	The performance metrics include: <ul style="list-style-type: none"> ■ Status ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms) 	The performance metrics include: <ul style="list-style-type: none"> ■ Most Popular Operations ■ Response Time ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms) ■ Maximum Time (ms) (Since Startup only)
Instant Messaging and Presence (IMP)	The performance metrics include: <ul style="list-style-type: none"> ■ Status ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms) 	The performance metrics include: <ul style="list-style-type: none"> ■ Most Popular Operations ■ Response Time ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms) ■ Maximum Time (ms) (Since Startup only)

Table 38–1 (Cont.) Common Performance Metrics

Service	Services Summary (Since Startup and Recent History)	Per Operation Metrics (Since Startup and Recent History)
Lists	<p>The performance metrics include:</p> <ul style="list-style-type: none"> ■ Status ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms) 	<p>The performance metrics include:</p> <ul style="list-style-type: none"> ■ Most Popular Operations ■ Response Time ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms) ■ Maximum Time (ms) (Since Startup only)
Mail	<p>The performance metrics include:</p> <ul style="list-style-type: none"> ■ Status ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms) 	<p>The performance metrics include:</p> <ul style="list-style-type: none"> ■ Most Popular Operations ■ Response Time ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms) ■ Maximum Time (ms) (Since Startup only)
Notes	<p>The performance metrics include:</p> <ul style="list-style-type: none"> ■ Status ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms) 	<p>The performance metrics include:</p> <ul style="list-style-type: none"> ■ Most Popular Operations ■ Response Time ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms) ■ Maximum Time (ms) (Since Startup only)
Pages	<p>The performance metrics include:</p> <ul style="list-style-type: none"> ■ Status ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms) 	<p>The performance metrics include:</p> <ul style="list-style-type: none"> ■ Most Popular Operations ■ Response Time ■ Successful Invocations (%) ■ Invocations ■ Average Time (ms) ■ Maximum Time (ms) (Since Startup only)

Table 38–1 (Cont.) Common Performance Metrics

Service	Services Summary (Since Startup and Recent History)	Per Operation Metrics (Since Startup and Recent History)
People Connections	<p>The performance metrics include:</p> <ul style="list-style-type: none"> ▪ Average Processing Time (ms) ▪ Invocations ▪ Successful Invocations (%) 	<p>The performance metrics include:</p> <ul style="list-style-type: none"> ▪ Most Popular Operations ▪ Response Time ▪ Successful Invocations (%) ▪ Invocations ▪ Average Time (ms) ▪ Maximum Time (ms) (Since Startup only)
Polls	<p>The performance metrics include:</p> <ul style="list-style-type: none"> ▪ Average Processing Time (ms) ▪ Invocations ▪ Successful Invocations (%) 	<p>The performance metrics include:</p> <ul style="list-style-type: none"> ▪ Most Popular Operations ▪ Response Time ▪ Successful Invocations (%) ▪ Invocations ▪ Average Time (ms) ▪ Maximum Time (ms) (Since Startup only)
Recent Activity	<p>The performance metrics include:</p> <ul style="list-style-type: none"> ▪ Average Time (ms) ▪ Successful Invocations (%) ▪ Invocations 	Not available
RSS	<p>The performance metrics include:</p> <ul style="list-style-type: none"> ▪ Status ▪ Successful Invocations (%) ▪ Invocations ▪ Average Time (ms) 	Not available
Search	<p>The performance metrics include:</p> <ul style="list-style-type: none"> ▪ Status ▪ Successful Invocations (%) ▪ Invocations ▪ Average Time (ms) 	<p>The performance metrics include:</p> <ul style="list-style-type: none"> ▪ Most Popular Operations ▪ Response Time ▪ Successful Invocations (%) ▪ Invocations ▪ Average Time (ms) ▪ Maximum Time (ms) (Since Startup only)

Table 38–2 describes metrics used for monitoring performance of all operations.

Table 38–2 Description of Common Metrics - Summary (All Operations)

Metric	Description
Status	<p>The current status of the service:</p> <ul style="list-style-type: none"> ■ Up (Green Up Arrow) - Indicates that a service is up and running and the last operation was successful. ■ Down (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. ■ Unknown (Clock) - Indicates that a service cannot query the status of the WebCenter Portal application for some reason.
Successful Invocations (%)	<p>Percentage of a service invocations that succeeded. Successful Invocations (%) equals the number of successful invocations divided by the invocation count:</p> <ul style="list-style-type: none"> - Since Startup - Recent History <p>If Successful Invocations (%) is below 100%, check the diagnostic logs to establish why service requests are failing. See, Section 38.3, "Viewing and Configuring Log Information".</p>
Invocations	<p>This metric shows number of service invocations per minute:</p> <ul style="list-style-type: none"> - Since Startup - Recent History <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 WebCenter Portal 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 with the Invocations metric to assess the total time spent in processing service operations.</p> <ul style="list-style-type: none"> - Since Startup - Recent History

[Table 38–3](#) describes metrics used to monitor performance of each operation performed by a service or component.

Table 38–3 Description of Common Metrics - Per Operation

Metric	Description
Most Popular Operations	<p>The number of invocations per operation (displayed on a chart). The highest value on the chart indicates which operation is used the most. 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 Portal application started up (displayed on a chart). The highest value on the chart indicates the worst performing operation. The lowest value indicates which operation is performing the best.</p>
Operation	<p>The operation being monitored. See also Section 38.1.4, "WebCenter Portal Service-Specific Metrics".</p>

Table 38–3 (Cont.) Description of Common Metrics - Per Operation

Metric	Description
Invocations	The number of invocations, per operation: - Since Startup - Recent History 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 WebCenter Portal services in the application.
Average Time (ms)	The average time taken to process each operation: - Since Startup - Recent History
Maximum Time (ms)	The maximum time taken to process each operation.

38.1.3 Common WebCenter Portal Performance Issues and Actions

This section provides information about identifying generic performance-related issues.

If a metric is out-of-bounds, 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 systemwide 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 a long time, 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 Portal 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. For details, refer to the "Testing Connection" section in the relevant chapter. For a list of chapters, see [Part IV, "Managing Services, Portlet Producers, and External Applications"](#).

If a service is reconfigured, but the container is not restarted to pick up the changes, then the service becomes unavailable.

38.1.4 WebCenter Portal Service-Specific Metrics

This section describes *per operation* metrics for all services and components. This section includes the following sub sections:

- [Section 38.1.4.1, "Announcement Metrics"](#)
- [Section 38.1.4.2, "BPEL Worklist Metrics"](#)
- [Section 38.1.4.3, "Content Repository Metrics"](#)
- [Section 38.1.4.4, "Discussion Metrics"](#)

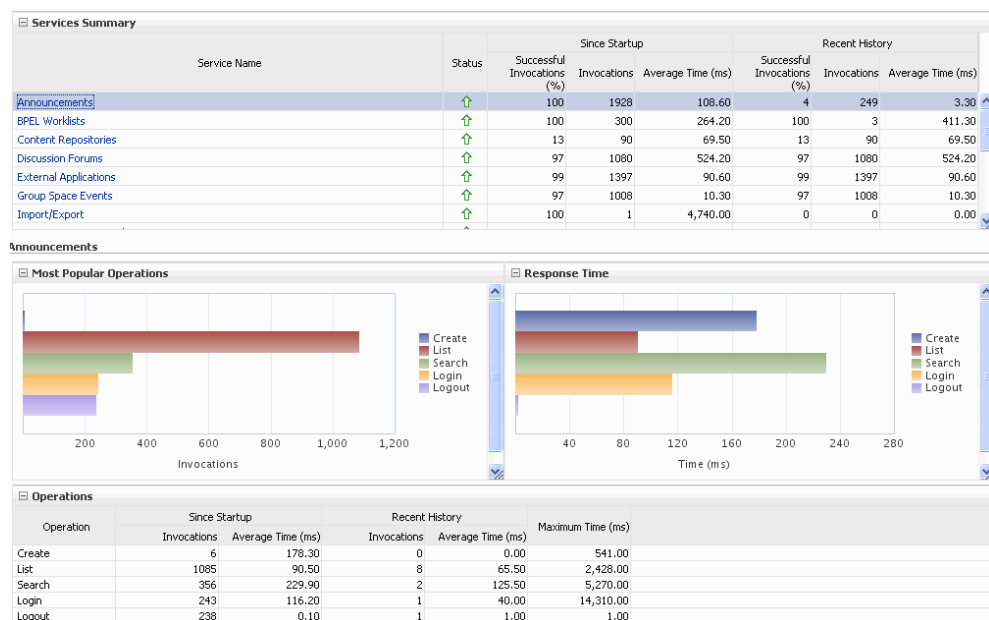
- [Section 38.1.4.6, "External Application Metrics"](#)
- [Section 38.1.4.5, "Events Metrics"](#)
- [Section 38.1.4.7, "Instant Messaging and Presence \(IMP\) Metrics"](#)
- [Section 38.1.4.8, "Import and Export Metrics"](#)
- [Section 38.1.4.9, "List Metrics"](#)
- [Section 38.1.4.10, "Mail Metrics"](#)
- [Section 38.1.4.11, "Note Metrics"](#)
- [Section 38.1.4.12, "Page Metrics"](#)
- [Section 38.1.4.13, "Portlet Producer Metrics"](#)
- [Section 38.1.4.14, "Portlet Metrics"](#)
- [Section 38.1.4.15, "People Connection Metrics"](#)
- [Section 38.1.4.16, "Poll Metrics"](#)
- [Section 38.1.4.17, "RSS News Feed Metrics"](#)
- [Section 38.1.4.18, "Recent Activity Metrics"](#)
- [Section 38.1.4.19, "Search Metrics"](#)

To access live performance metrics for your WebCenter Portal application, see [Section 38.2, "Viewing Performance Information."](#)

38.1.4.1 Announcement Metrics

Performance metrics associated with the Announcements service ([Figure 38–1](#)) are described in [Table 38–4](#) and [Section 38.1.2, "Common WebCenter Portal Metrics."](#)

Figure 38–1 *Announcement Metrics*



To monitor these metrics through Fusion Middleware Control, see [Section 38.2, "Viewing Performance Information."](#)

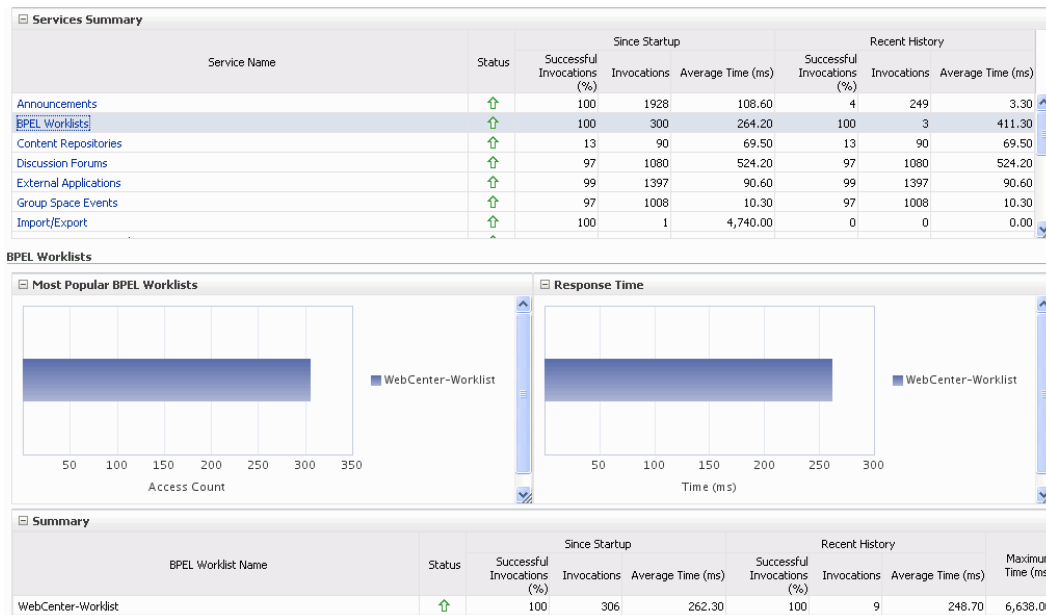
Table 38–4 Announcements Service - Operations Monitored

Operation	Description	Performance Issues - User Action
Login	Logs a WebCenter Portal user (accessing the Announcements service) into the discussions server that is hosting announcements.	For service-specific causes, see Section 38.1.5.1, "Announcements Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Logout	Logs a WebCenter Portal user out of the discussions server that is hosting announcements.	For service-specific causes, see Section 38.1.5.1, "Announcements Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Search	Searches for terms within announcement text.	If Announcement searches are failing, verify that Announcement text contains the search terms. For other causes, see Section 38.1.5.1, "Announcements Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Create	Creates an announcement.	For service-specific causes, see Section 38.1.5.1, "Announcements Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
List	Retrieves a list of announcements.	For service-specific causes, see Section 38.1.5.1, "Announcements Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."

38.1.4.2 BPEL Worklist Metrics

Performance metrics associated with the BPEL Worklist service ([Figure 38–2](#)) are described in [Section 38.1.2, "Common WebCenter Portal Metrics."](#)

Figure 38–2 BPEL Worklist Metrics



To monitor these metrics through Fusion Middleware Control, see [Section 38.2, "Viewing Performance Information."](#)

38.1.4.3 Content Repository Metrics

Performance metrics associated with the Documents service and Content Presenter (Figure 38–3 and Figure 38–4) are described in the following tables:

- [Table 38–5, "Content Repository - Operations Monitored"](#)
- [Table 38–6, "Content Repository Metrics - Summary \(All Repositories\)"](#)
- [Table 38–7, "Content Repository Metrics - Operation Summary Per Repository"](#)
- [Table 38–8, "Content Repository Metrics - Operation Detail Per Repository"](#)

Figure 38–3 Content Repository Metrics

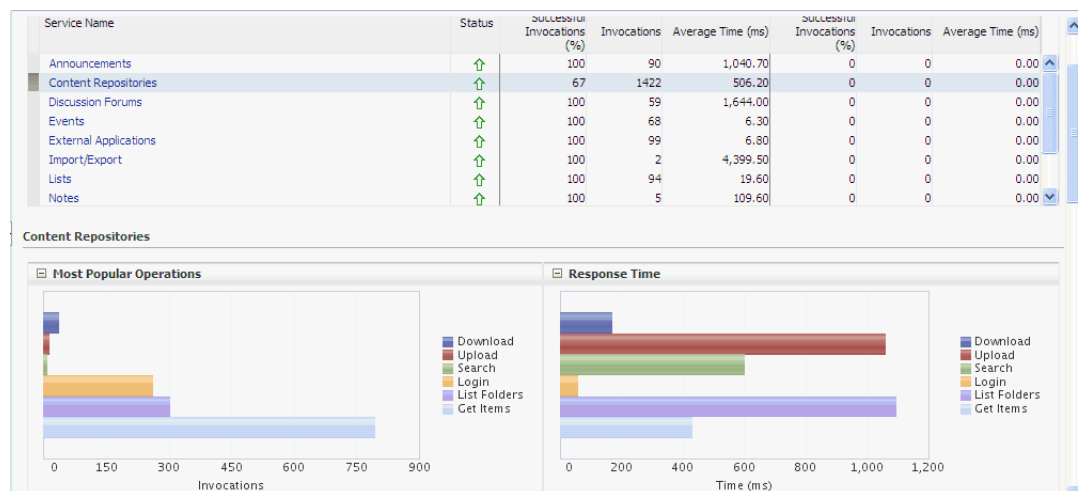
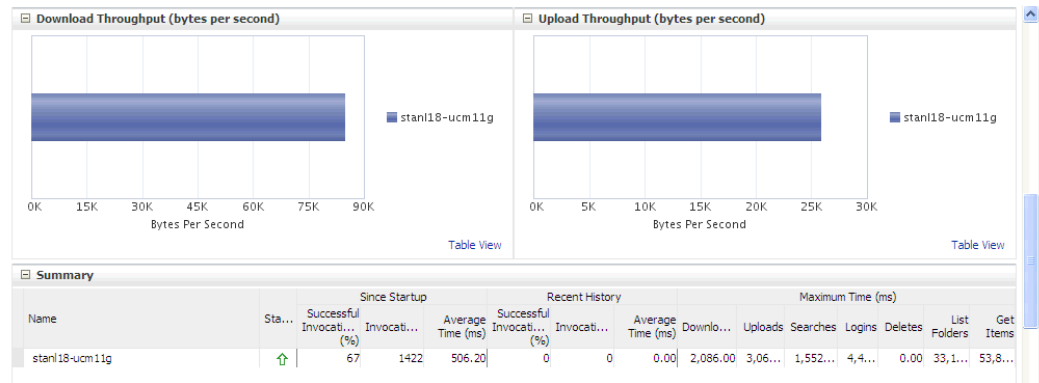


Figure 38–4 Content Repository Metrics - Per Operation



To monitor these metrics through Fusion Middleware Control, see [Section 38.2, "Viewing Performance Information."](#)

Table 38–5 Content Repository - Operations Monitored

Operation	Description	Performance Issues - User Action
Download	Downloads one or more documents from a content repository.	<p>For service-specific causes, see Section 38.1.5.3, "Content Repository (Documents and Content Presenter) Service."</p> <p>For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."</p>
Upload	Uploads one or more documents to a content repository.	<p>For service-specific causes, see Section 38.1.5.3, "Content Repository (Documents and Content Presenter) Service."</p> <p>For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."</p>
Search	Searches for documents stored in a content repository.	<p>For service-specific causes, see Section 38.1.5.3, "Content Repository (Documents and Content Presenter) Service."</p> <p>For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."</p>
Login	Establishes a connection to the content repository and authenticates the user.	<p>For service-specific causes, see Section 38.1.5.3, "Content Repository (Documents and Content Presenter) Service."</p> <p>For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."</p>

Table 38–5 (Cont.) Content Repository - Operations Monitored

Operation	Description	Performance Issues - User Action
Delete	Deletes one or more documents stored in a content repository.	For service-specific causes, see Section 38.1.5.3, "Content Repository (Documents and Content Presenter) Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
List Folders	Lists folders stored in a content repository. This operation is specific to Content Presenter.	For service-specific causes, see Section 38.1.5.3, "Content Repository (Documents and Content Presenter) Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Get Items	Displays items, such as a document or image stored in a content repository. This operation is specific to Content Presenter.	For service-specific causes, see Section 38.1.5.3, "Content Repository (Documents and Content Presenter) Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."

Table 38–6 Content Repository Metrics - Summary (All Repositories)

Metric	Description
Status	<p>The current status of the Documents service:</p> <ul style="list-style-type: none"> ■ Up (Green Up Arrow) - Indicates that the Documents service is up and running and the last operation was successful. ■ Down (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 Down. <p>If you are having problems with the Documents service, check the diagnostic logs to establish why this service is "Down". See Section 38.3, "Viewing and Configuring Log Information."</p> <p>Some typical causes of failure include:</p> <ul style="list-style-type: none"> - Content repository is down or not responding. - Network connectivity issues exist between the application and one or more content repositories. - Connection configuration information associated with one or more content repositories is incorrect or no longer valid. <ul style="list-style-type: none"> ■ Clock - Unable to query the status of the service for some reason.

Table 38–6 (Cont.) Content Repository Metrics - Summary (All Repositories)

Metric	Description
Successful Invocations (%)	<p>The percentage of Documents service invocations that succeeded (Upload, Download, Search Login, Delete):</p> <ul style="list-style-type: none"> - Since Startup - Recent History <p>If Successful Invocations (%) is below 100%, check the diagnostic logs to establish why service requests are failing. See, Section 38.3, "Viewing and Configuring Log Information."</p>
Invocations	<p>The number of Documents service invocations per minute (Upload, Download, Search Login, Delete):</p> <ul style="list-style-type: none"> - Since Startup - Recent History <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 WebCenter Portal service 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"> - Since Startup - Recent History
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 Portal 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 38–7 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"> ■ Up (Green Up Arrow) - Indicates that the content repository is up and running and the last operation was successful. ■ Down (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 Down. <p>If you are having problems with a content repository, check the diagnostic logs to establish why this service is "Down". See, Section 38.3, "Viewing and Configuring Log Information."</p> <p>Some typical causes of failure include:</p> <ul style="list-style-type: none"> - Content repository is down or not responding. - Network connectivity issues exist between the application and one or more content repositories. - Connection configuration information associated with one or more content repositories is incorrect or no longer valid. <ul style="list-style-type: none"> ■ Clock - Unable to query the status of the service for some reason.
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"> - Since Startup - Recent History <p>If Successful Invocations (%) is below 100%, check the diagnostic logs to establish why service requests are failing. See, Section 38.3, "Viewing and Configuring Log Information".</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"> - Since Startup - Recent History <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 WebCenter Portal service 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) for this content repository:</p> <ul style="list-style-type: none"> - Since Startup - Recent History
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 38–7 (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.

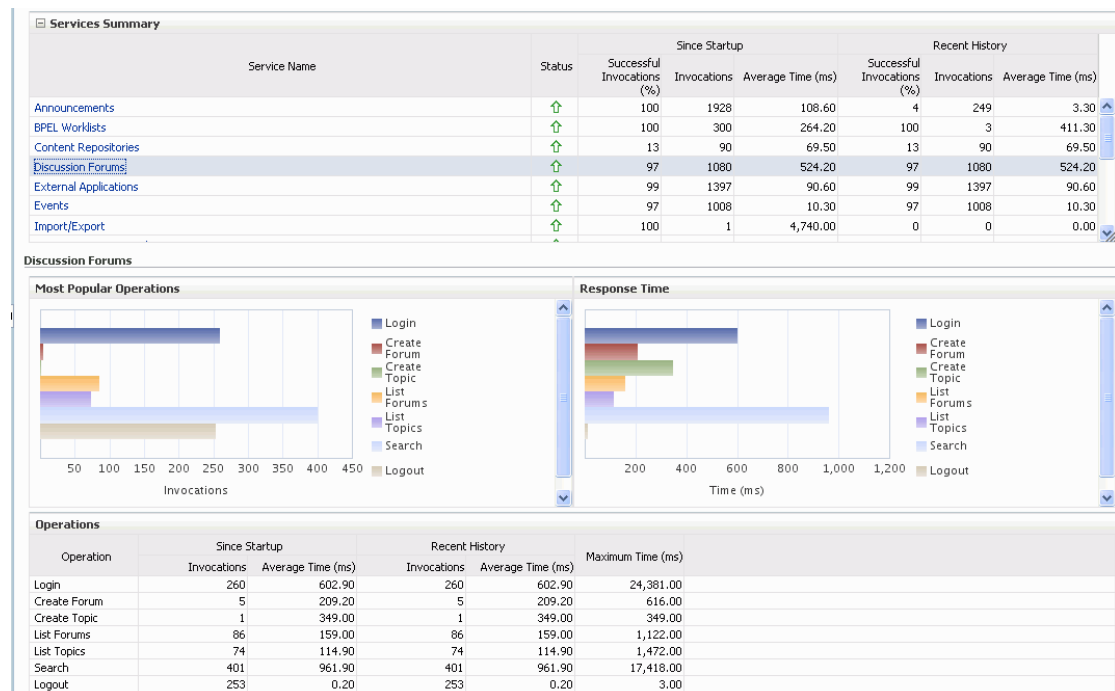
Table 38–8 Content Repository Metrics - Operation Detail Per Repository

Metric	Description
Invocations	<p>The number of Documents service invocations per operation (Upload, Download, Search, Login, Delete):</p> <ul style="list-style-type: none"> - Since Startup - Recent History <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 WebCenter Portal service 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"> - Since Startup - Recent History

38.1.4.4 Discussion Metrics

Performance metrics associated with the Discussions service (Figure 38–5) are described in Table 38–9 and Section 38.1.2, "Common WebCenter Portal Metrics."

Figure 38–5 Discussion Metrics



To monitor these metrics through Fusion Middleware Control, see [Section 38.2, "Viewing Performance Information."](#)

Table 38–9 Discussions Service - Operations Monitored

Operation	Description	Performance Issues - User Action
Login	Logs a WebCenter Portal user (accessing the Discussions service) into the discussions server that is hosting discussions forums.	<p>For service-specific causes, see Section 38.1.5.4, "Discussions Service."</p> <p>For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."</p>
Logout	Logs a WebCenter Portal user out of the discussions server that is hosting discussion forums.	<p>For service-specific causes, see Section 38.1.5.4, "Discussions Service."</p> <p>For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."</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"> ■ Category under which discussion forums must be created has been deleted. ■ User does not have permissions to create discussion forums. <p>For other service-specific causes, see Section 38.1.5.4, "Discussions Service."</p> <p>For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."</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"> ■ Discussion forum under which topics must be created has been deleted. ■ User does not have permissions to create topics. <p>For other service-specific causes, see Section 38.1.5.4, "Discussions Service".</p> <p>For information on common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions".</p>

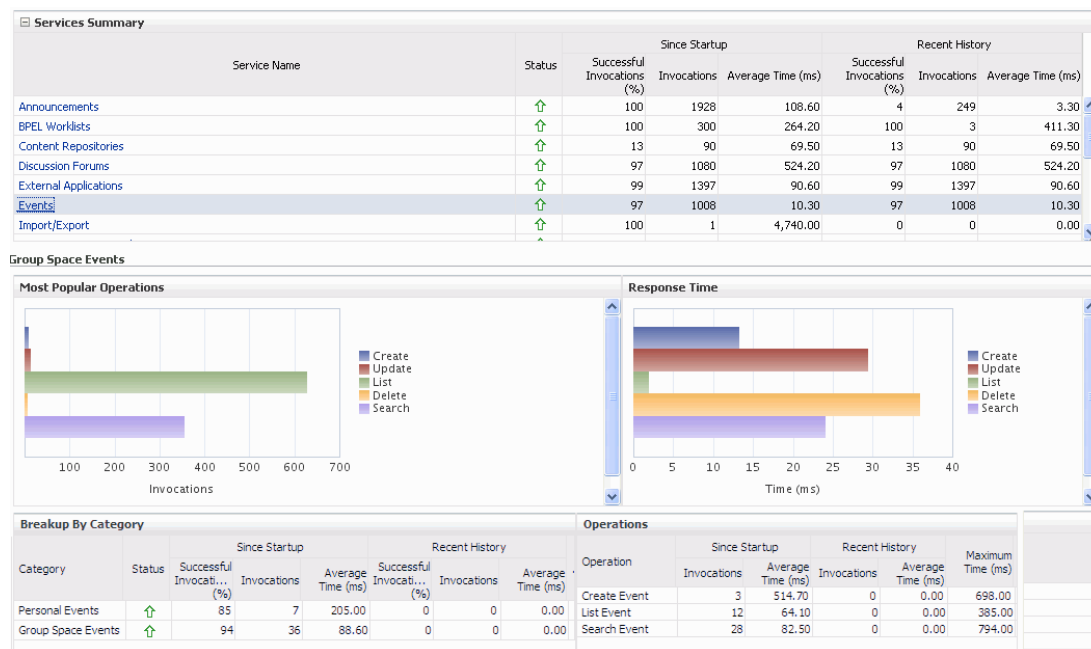
Table 38–9 (Cont.) Discussions Service - Operations Monitored

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"> ■ User does not have permissions to view forums in the category. ■ Category from which to fetch forums has been deleted. <p>For other service-specific causes, see Section 38.1.5.4, "Discussions Service."</p> <p>For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."</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"> ■ User does not have permissions to view topics in the forum. ■ Forum from which to fetch topics has been deleted. <p>For other service-specific causes, see Section 38.1.5.4, "Discussions Service."</p> <p>For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."</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"> ■ No topic/messages exist with the specified search term. ■ Category or forum in which the search term object resides has been deleted. <p>For other service-specific causes, see Section 38.1.5.4, "Discussions Service."</p> <p>For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."</p>

38.1.4.5 Events Metrics

Performance metrics associated with the Events service are described in [Table 38–10](#) and [Section 38.1.2, "Common WebCenter Portal Metrics."](#)

Figure 38–6 Events Metrics



To monitor these metrics through Fusion Middleware Control, see [Section 38.2, "Viewing Performance Information."](#)

Table 38–10 Events Service - Operations Monitored

Operation	Description	Performance Issues - User Action
Create Event	Creates a space or personal event in the WebCenter Portal's repository.	For service-specific causes, see Section 38.1.5.6, "Events Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Update Event	Updates a space or personal event stored in the WebCenter Portal's repository.	For service-specific causes, see Section 38.1.5.6, "Events Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Delete Event	Deletes a space or personal event in the WebCenter Portal's repository.	For service-specific causes, see Section 38.1.5.6, "Events Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
List Event	Retrieves a list of events from the WebCenter Portal's repository.	For service-specific causes, see Section 38.1.5.6, "Events Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."

Table 38–10 (Cont.) Events Service - Operations Monitored

Operation	Description	Performance Issues - User Action
Search Event	Searches for terms within event text.	For service-specific causes, see Section 38.1.5.6, "Events Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."

38.1.4.6 External Application Metrics

Performance metrics associated with the External Application service are described in [Table 38–11](#) and [Section 38.1.2, "Common WebCenter Portal Metrics."](#)

Figure 38–7 External Application Metrics

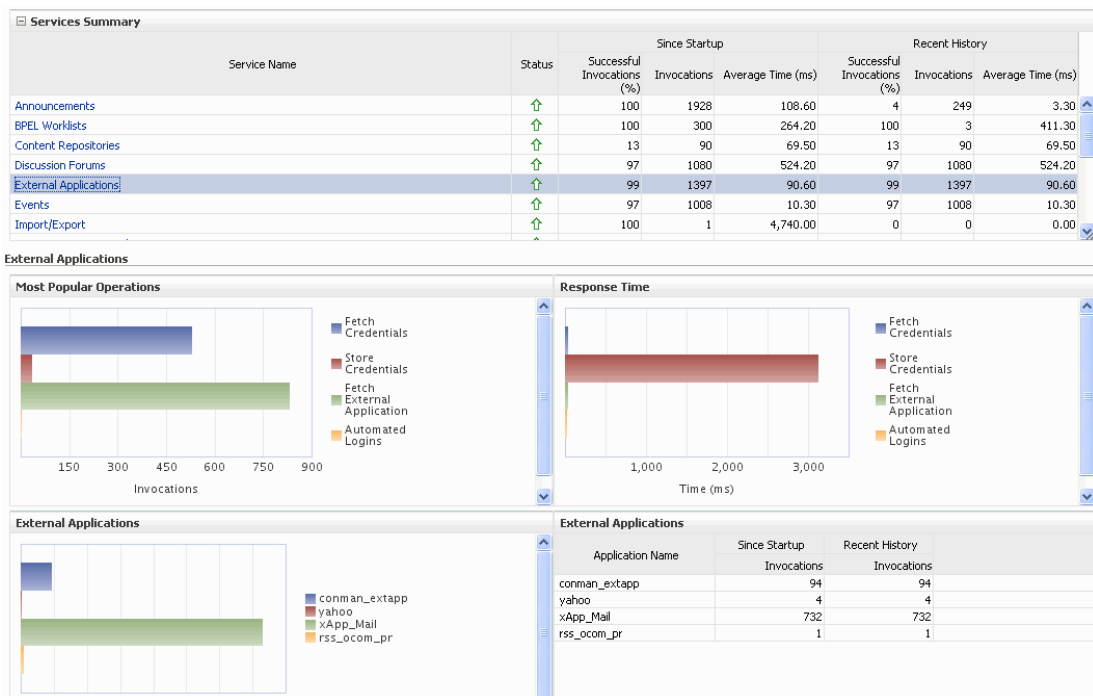
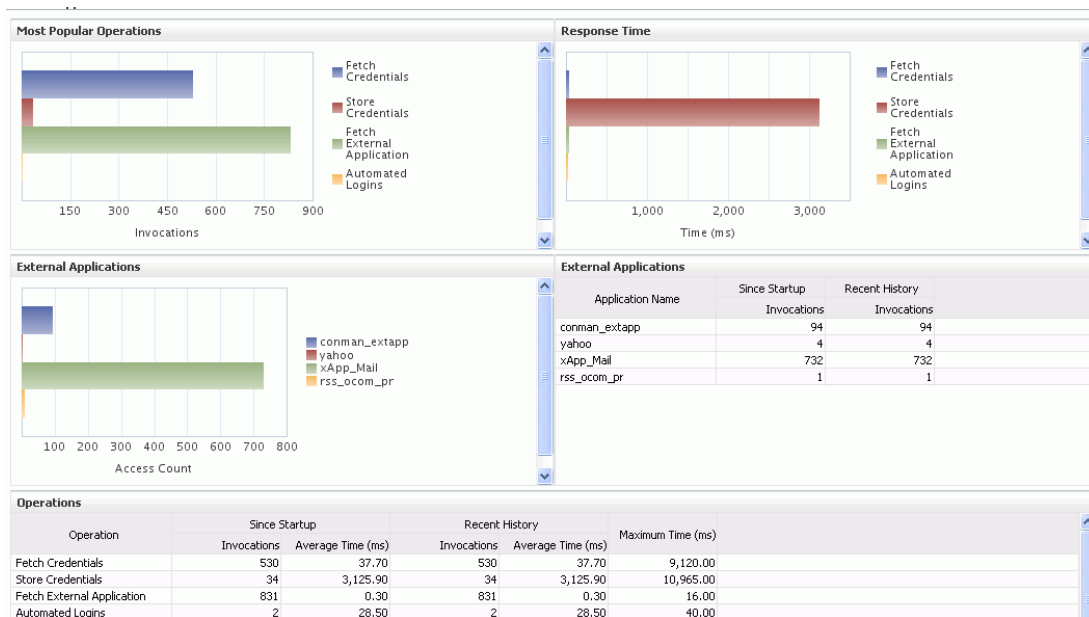


Figure 38–8 External Application Metrics - Per Operation



To monitor these metrics through Fusion Middleware Control, see [Section 38.2, "Viewing Performance Information."](#)

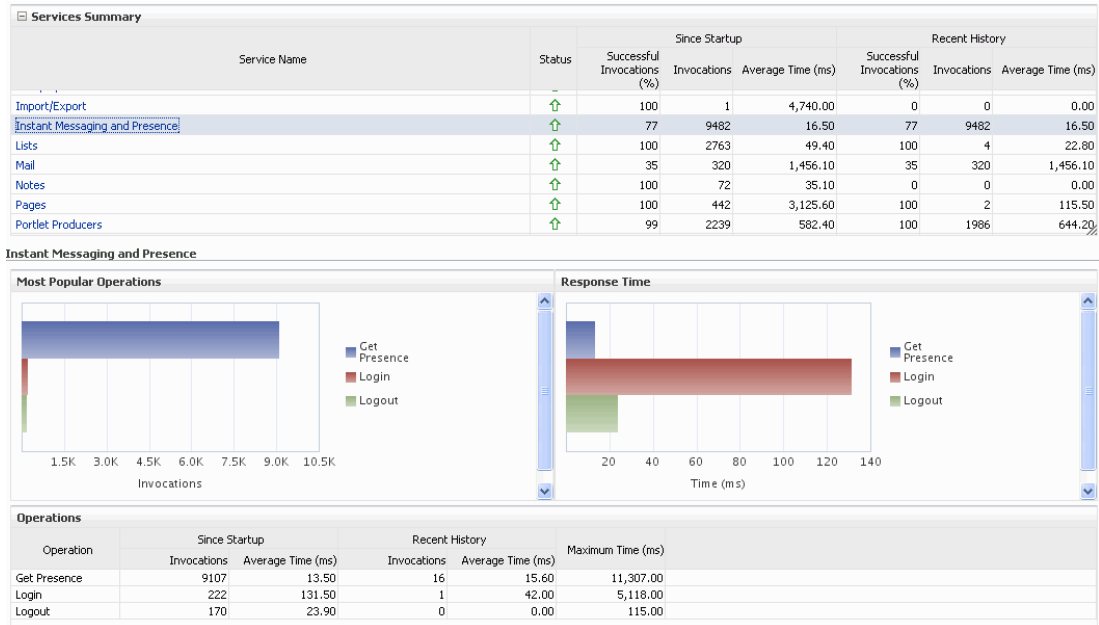
Table 38–11 External Applications - Operations Monitored

Operation	Description	Performance Issues - User Action
Fetch Credentials	Retrieves credentials for an external application.	For service-specific causes, see Section 38.1.5.5, "External Applications Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Store Credentials	Stores user credentials for an external application.	For service-specific causes, see Section 38.1.5.5, "External Applications Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Fetch External Application	Retrieves an external application.	For service-specific causes, see Section 38.1.5.5, "External Applications Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Automated Logins	Logs a WebCenter Portal user in to an external application (using the automated login feature).	For service-specific causes, see Section 38.1.5.5, "External Applications Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."

38.1.4.7 Instant Messaging and Presence (IMP) Metrics

Performance metrics associated with the Instant Messaging and Presence (IMP) service (Figure 38–9) are described in Table 38–12 and Section 38.1.2, "Common WebCenter Portal Metrics."

Figure 38–9 IMP Metrics



To monitor these metrics through Fusion Middleware Control, see Section 38.2, "Viewing Performance Information."

Table 38–12 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 38.1.5.7, "Instant Messaging and Presence (IMP) Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Login	Logs a WebCenter Portal user (accessing the IMP service) into the IMP server.	For service-specific causes, see Section 38.1.5.7, "Instant Messaging and Presence (IMP) Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Logout	Logs a WebCenter Portal user (accessing the IMP service) out of the IMP server.	For service-specific causes, see Section 38.1.5.7, "Instant Messaging and Presence (IMP) Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."

38.1.4.8 Import and Export Metrics

Performance metrics associated with import and export services (Figure 38–10) are described in Table 38–13 and Section 38.1.2, "Common WebCenter Portal Metrics." These metrics apply to Spaces only.

Figure 38–10 Import/Export Metrics

The screenshot shows two tables from the Oracle WebCenter Portal interface. The top table, titled "Services Summary", lists various services with their status and performance metrics. The bottom table, titled "Import/Export Summary", provides a detailed view of the Import and Export operations.

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 38.2, "Viewing Performance Information."

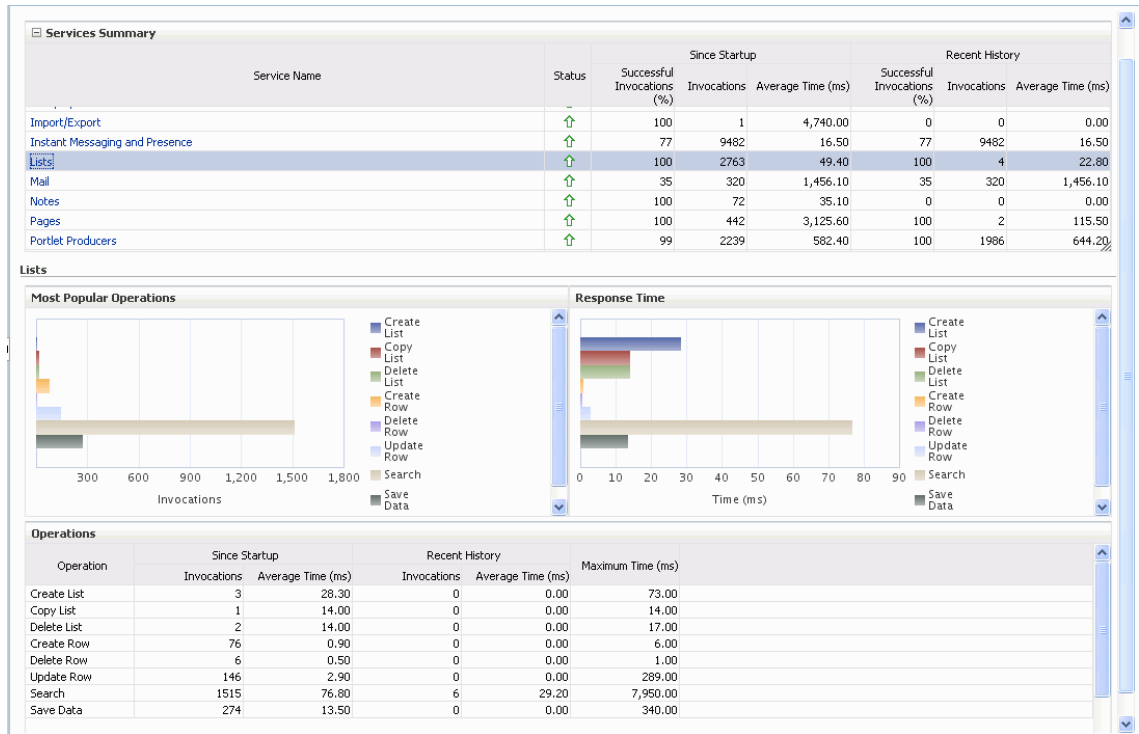
Table 38–13 Import/Export - Operations Monitored

Operation	Description	Performance Issues - User Action
Export	Exports an entire WebCenter Portal application.	For service-specific causes, see Section 38.1.5.8, "Import and Export." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Import	Imports entire WebCenter Portal application.	For service-specific causes, see Section 38.1.5.8, "Import and Export." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."

38.1.4.9 List Metrics

(WebCenter Portal: Spaces only) Performance metrics associated with the List service (Figure 38–11) are described in Table 38–14 and Section 38.1.2, "Common WebCenter Portal Metrics."

Figure 38–11 List Metrics



To monitor these metrics through Fusion Middleware Control, see [Section 38.2, "Viewing Performance Information."](#)

Table 38–14 List service - Operations Monitored

Operation	Description	Performance Issues - User Action
Create List	Creates a list in the user session.	For service-specific causes, see Section 38.1.5.9, "Lists Service."
	The Save Data operation commits new lists to the MDS repository.	For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Copy List	Copies a list and its data in the user session.	For service-specific causes, see Section 38.1.5.9, "Lists Service."
	The Save Data operation commits copied lists and list data to the MDS repository and the WebCenter Portal's repository (the database where list data is stored).	For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Delete List	Deletes a list and its data in the user session.	For service-specific causes, see Section 38.1.5.9, "Lists Service."
	The Save Data operation commits list changes to the MDS repository and the WebCenter Portal's repository (the database where list data is stored).	For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."

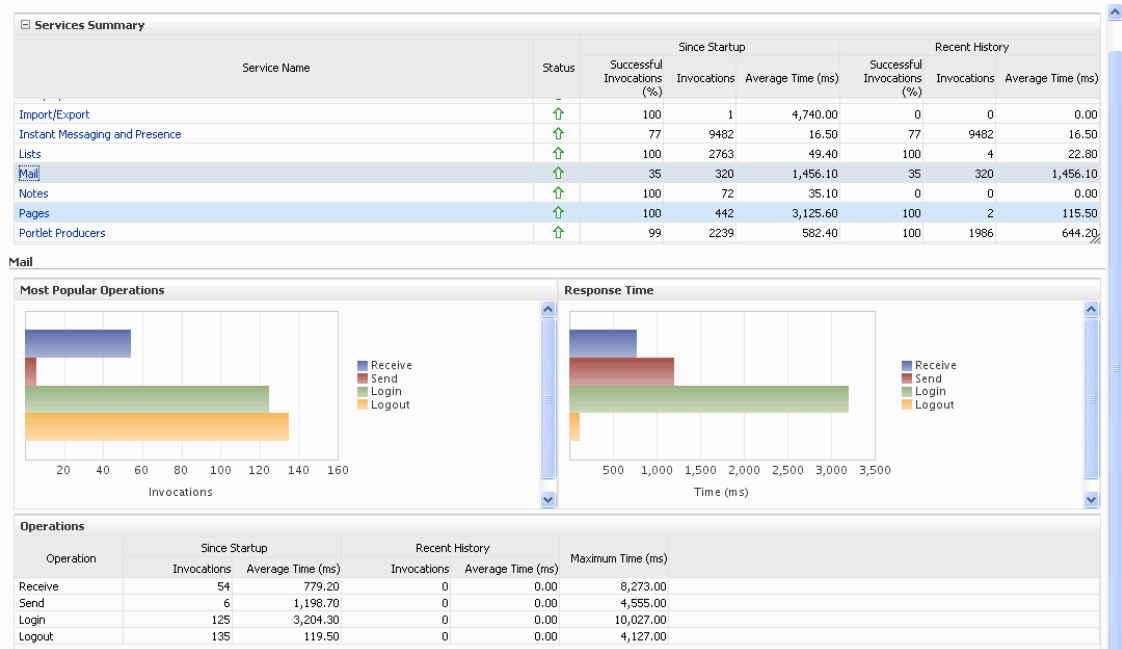
Table 38–14 (Cont.) List service - Operations Monitored

Operation	Description	Performance Issues - User Action
Create Row	Creates row of list data in the user session.	For service-specific causes, see Section 38.1.5.9, "Lists Service."
	The Save Data operation commits list data changes to the WebCenter Portal's repository (the database where list data is stored).	For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Update Row	Updates row of list data in the user session.	For service-specific causes, see Section 38.1.5.9, "Lists Service."
	The Save Data operation commits list data changes to the WebCenter Portal's repository (the database where list data is stored).	For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Delete Row	Deletes row of list data in the user session.	For service-specific causes, see Section 38.1.5.9, "Lists Service."
	The Save Data operation commits list data changes to the WebCenter Portal's repository (the database where list data is stored).	For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Search	Retrieves a list by its ID from the Metadata repository.	For service-specific causes, see Section 38.1.5.9, "Lists Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Save Data	Saves all changes to lists and list data (in the user session) to the Metadata Services repository and the WebCenter Portal's repository (the database where list information is stored).	For service-specific causes, see Section 38.1.5.9, "Lists Service."
		For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."

38.1.4.10 Mail Metrics

Performance metrics associated with the Mail service ([Figure 38–12](#)) are described in [Table 38–15](#) and [Section 38.1.2, "Common WebCenter Portal Metrics."](#)

Figure 38–12 Mail Metrics



To monitor these metrics through Fusion Middleware Control, see [Section 38.2, "Viewing Performance Information."](#)

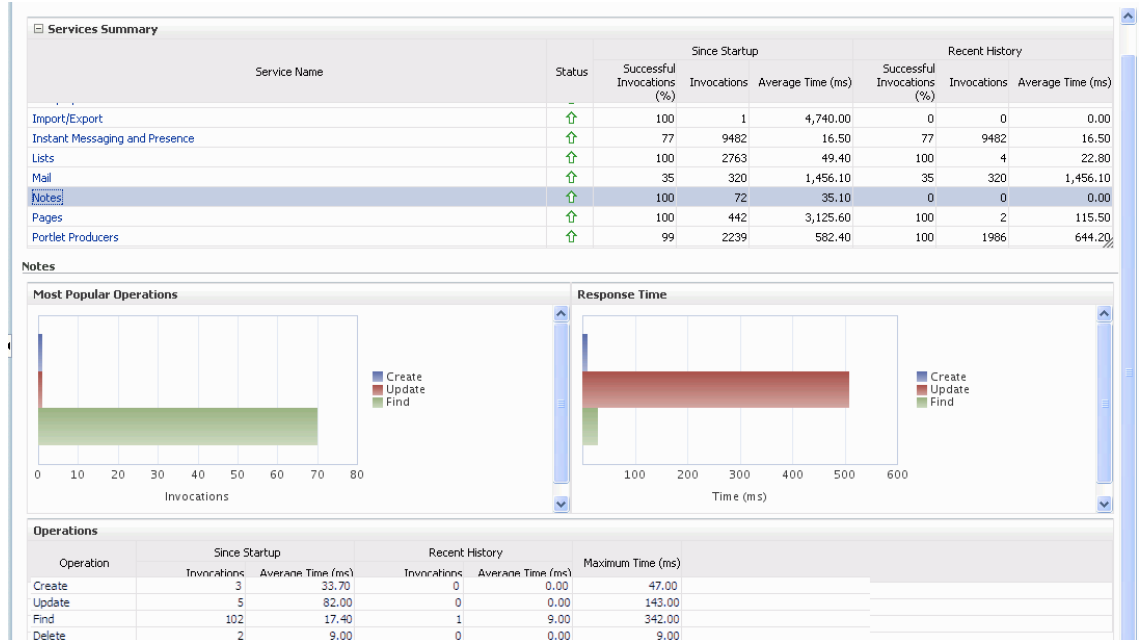
Table 38–15 Mail Service - Operations Monitored

Operation	Description	Performance Issues - User Action
Login	Logs a WebCenter Portal user into the mail server that is hosting mail services.	For service-specific causes, see Section 38.1.5.10, "Mail Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Logout	Logs a WebCenter Portal user out of the mail server that is hosting mail services.	For service-specific causes, see Section 38.1.5.10, "Mail Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Receive	Receives a mail.	For service-specific causes, see Section 38.1.5.10, "Mail Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Send	Sends a mail.	For service-specific causes, see Section 38.1.5.10, "Mail Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Search	Searches for mail that contains a specific term.	For service-specific causes, see Section 38.1.5.10, "Mail Service." For information on common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."

38.1.4.11 Note Metrics

Performance metrics associated with the Notes service (Figure 38–13) are described in Table 38–16 and Section 38.1.2, "Common WebCenter Portal Metrics."

Figure 38–13 Notes Metrics



To monitor these metrics through Fusion Middleware Control, see Section 38.2, "Viewing Performance Information."

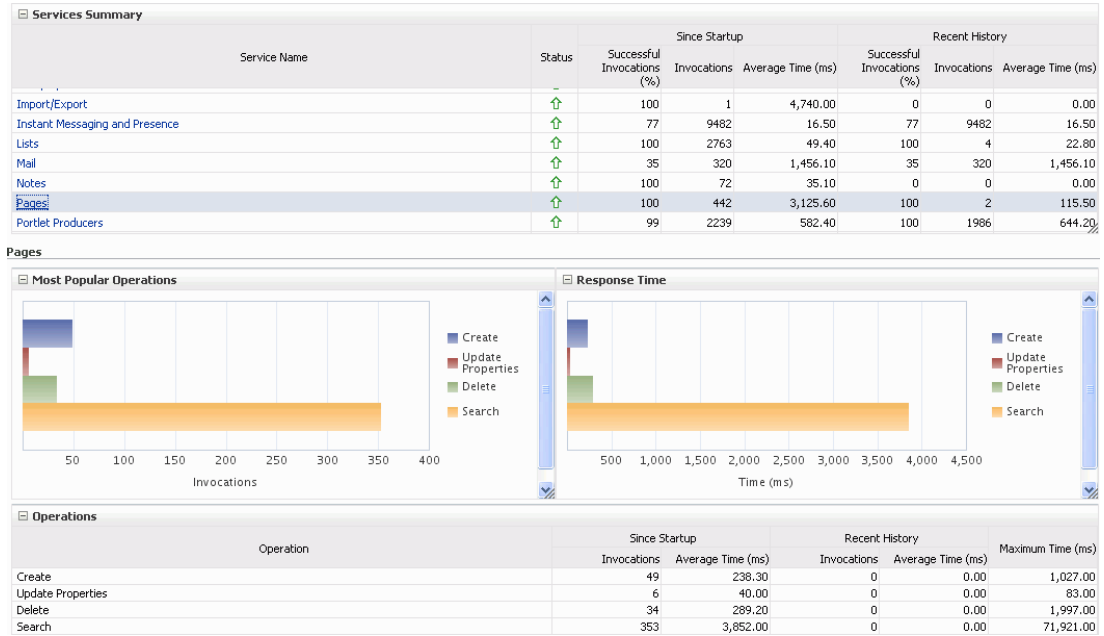
Table 38–16 Notes Service - Operations Monitored

Operation	Description	Performance Issues - User Action
Create	Creates a personal note. The Save Changes operation commits new notes to the MDS repository.	For service-specific causes, see Section 38.1.5.11, "Notes Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Update	Updates a personal note. The Save Changes operation commits note updates to the MDS repository.	For service-specific causes, see Section 38.1.5.11, "Notes Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Find	Retrieves a note from the MDS repository.	For service-specific causes, see Section 38.1.5.11, "Notes Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Delete	Deletes a note from the MDS repository.	For service-specific causes, see Section 38.1.5.11, "Notes Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."

38.1.4.12 Page Metrics

Performance metrics associated with the Page service (Figure 38–14) are described in Table 38–17 and Section 38.1.2, "Common WebCenter Portal Metrics."

Figure 38–14 Page Metrics



To monitor these metrics through Fusion Middleware Control, see Section 38.2, "Viewing Performance Information."

Table 38–17 Page Service - Operations Monitored

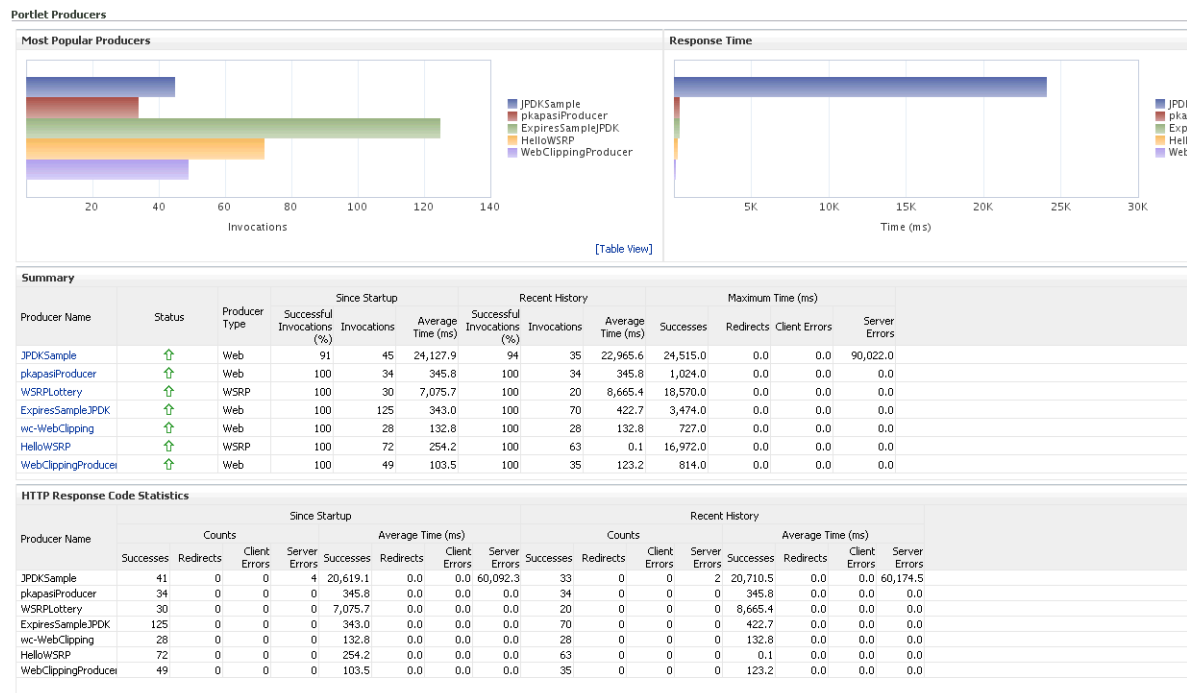
Operation	Description	Performance Issues - User Action
Create	Creates a page in the WebCenter Portal application.	For service-specific causes, see Section 38.1.5.12, "Page Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Copy	Copies a page.	For service-specific causes, see Section 38.1.5.12, "Page Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Delete	Deletes a page.	For service-specific causes, see Section 38.1.5.12, "Page Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Search	Searches for pages that contain a specific term.	For service-specific causes, see Section 38.1.5.12, "Page Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."

38.1.4.13 Portlet Producer Metrics

Performance metrics associated with the portlet producers (Figure 38–15) are described in the following tables:

- Table 38–18, "Portlet Producers - Summary"
- Table 38–19, "Portlet Producer - Detail"

Figure 38–15 Portlet Producer Metrics



To monitor these metrics through Fusion Middleware Control, see Section 38.2, "Viewing Performance Information."

Table 38–18 Portlet Producers - Summary

Metric	Description
Status	<p>The current status of portlet producers used in the WebCenter Portal application:</p> <ul style="list-style-type: none"> ■ Up (Green Up Arrow) - Indicates that all portlet producers are up and running. ■ Down (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. ■ Clock - Unable to query the status of the portlet producers for some reason.

Table 38–18 (Cont.) Portlet Producers - Summary

Metric	Description
Successful Invocations (%)	<p>The percentage of portlet producer invocations that succeeded:</p> <ul style="list-style-type: none"> - Since Startup - Recent History <p>Any request that fails will impact availability. This includes WebCenter Portal application-related failures such as timeouts and internal errors, and also client/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, Section 38.3, "Viewing and Configuring Log Information."</p>
Invocations	<p>The number of portlet producer invocations per minute:</p> <ul style="list-style-type: none"> - Since Startup - Recent History <p>This metric measures each WebCenter Portal 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"> - Since Startup - Recent History

Table 38–19 Portlet Producer - Detail

Metric	Description
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 Portal 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 Table 38–21, "Portlet - Detail".</p>

Table 38–19 (Cont.) Portlet Producer - Detail

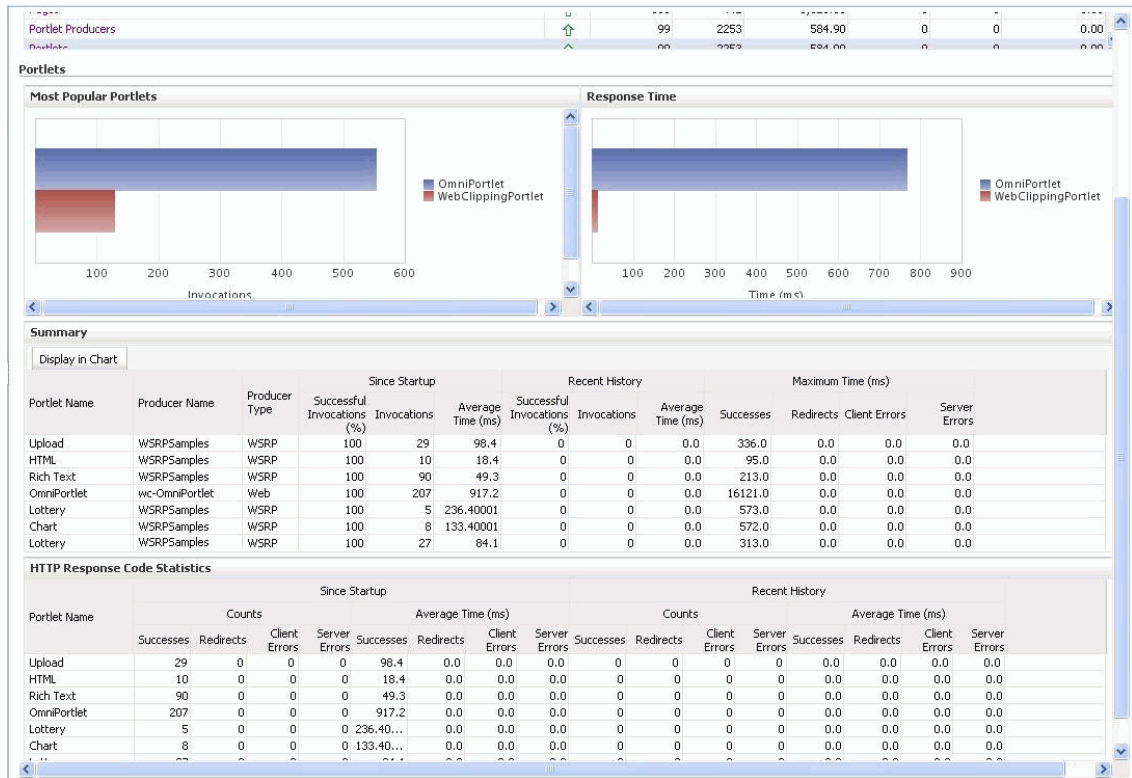
Metric	Description
Status	<p>The current status of each portlet producer:</p> <ul style="list-style-type: none"> ■ Up (Green Up Arrow) - Indicates that the portlet producer is up and running. ■ Down (Red Down Arrow) - Indicates that the portlet producer is currently unavailable. The producer instance might be down, or there could be some network connectivity issues. ■ Clock - Unable to query the status of portlet producer for some reason.
Producer Type	<p>The portlet producer type: Web or WSRP</p> <ul style="list-style-type: none"> ■ Web portlet producer - deployed to a J2EE application server, which is often remote and communicates through Simple Object Access Protocol (SOAP) over HTTP. ■ 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.
Successful Invocations (%)	<p>The percentage of producer invocations that succeeded:</p> <ul style="list-style-type: none"> - Since Startup - Recent History
Invocations	<p>The number of invocations, per producer:</p> <ul style="list-style-type: none"> - Since Startup - Recent History <p>By sorting the table on this column, you can find the most frequently accessed portlet producer in your WebCenter Portal 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"> - Since Startup - Recent History <p>Use this metric to detect non-functional portlet producers. If you use this metric 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"> - Successes - HTTP200xx response code - Re-directs - HTTP300xx response code - Client Errors - HTTP400xx response code - Server Errors - HTTP500xx response code

38.1.4.14 Portlet Metrics

Performance metrics associated with portlets ([Figure 38–16](#)) are described in the following tables:

- [Table 38–20, "Portlets - Summary"](#)
- [Table 38–21, "Portlet - Detail"](#)
- [Table 38–22, "Portlet - HTTP Response Code Statistics"](#)
- [Table 38–23, "HTTP Response Codes"](#)

Figure 38–16 Portlet Metrics



To monitor these metrics through Fusion Middleware Control, see [Section 38.2, "Viewing Performance Information."](#)

Table 38–20 Portlets - Summary

Metric	Description
Status	<p>The current status of portlets used in the WebCenter Portal application:</p> <ul style="list-style-type: none"> ■ Up (Green Up Arrow) - Indicates that all portlets are up and running. ■ Down (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 Section 38.1.5.13, "Portlets and Producers." ■ Clock - Unable to query the status of portlets for some reason.
Successful Invocations (%)	<p>The percentage of portlet invocations that succeeded:</p> <ul style="list-style-type: none"> - Since Startup - Recent History <p>Any request that fails will impact availability. This includes WebCenter Portal application-related failures such as timeouts and internal errors, and also client/server errors.</p> <p>If Successful Invocations (%) is below 100%, check the diagnostic logs to establish why service requests are failing. See, Section 38.3, "Viewing and Configuring Log Information."</p>

Table 38–20 (Cont.) Portlets - Summary

Metric	Description
Invocations	The number of portlet invocations per minute: - Since Startup - Recent History This metric measures each WebCenter Portal 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.
Average Time (ms)	The average time taken to process operations associated with portlets, regardless of the result: - Since Startup - Recent History

Table 38–21 Portlet - Detail

Metric	Description
Most Popular Portlets	The number of invocations per portlet (displayed on a chart). The highest value on the chart indicates which portlet is used the most. The lowest value indicates which portlet is used the least.
Response Time	The average time each portlet takes to process requests since the WebCenter Portal application started up (displayed on a chart). The highest value on the chart indicates the worst performing portlet. The lowest value indicates which portlet is performing the best.
Portlet Name	The name of the portlet being monitored.
Status	The current status of each portlet: <ul style="list-style-type: none"> ■ Up (Green Up Arrow) - Indicates that the portlet is up and running. ■ Down (Red Down Arrow) - Indicates that the portlet is currently unavailable. The producer instance might be down, or there could be some network connectivity issues.
Producer Name	The name of the portlet producer through which the portlet is accessed.
Producer Type	The portlet producer type: Web or WSRP <ul style="list-style-type: none"> ■ Web portlet producer - deployed to a J2EE application server, which is often remote and communicates through Simple Object Access Protocol (SOAP) over HTTP. ■ 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.
Successful Invocations (%)	The percentage of portlet invocations that succeeded: - Since Startup - Recent History If Successful Invocations (%) is below 100%, check the diagnostic logs to establish why service requests are failing. See, Section 38.3, "Viewing and Configuring Log Information."

Table 38–21 (Cont.) Portlet - Detail

Metric	Description
Invocations	<p>The number of invocations, per portlet:</p> <ul style="list-style-type: none"> - Since Startup - Recent History <p>By sorting the table on this column, you can find the most frequently accessed portlet in your WebCenter Portal 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"> - Since Startup - Recent History <p>Use this metric to detect non-performant portlets. If you use this metric 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"> - Successes - HTTP200xx - Redirects - HTTP300xx - Client Errors - HTTP400xx - Server Errors - HTTP500xx <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 38–22 Portlet - HTTP Response Code Statistics

Metric	Description
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 Table 38–23, " HTTP Response Codes" .
- 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 with the Invocations metric, then you can prioritize which portlet to focus on.
- Server Errors	

Table 38–23 HTTP Response Codes

HTTP Response and Error Code	Description
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.

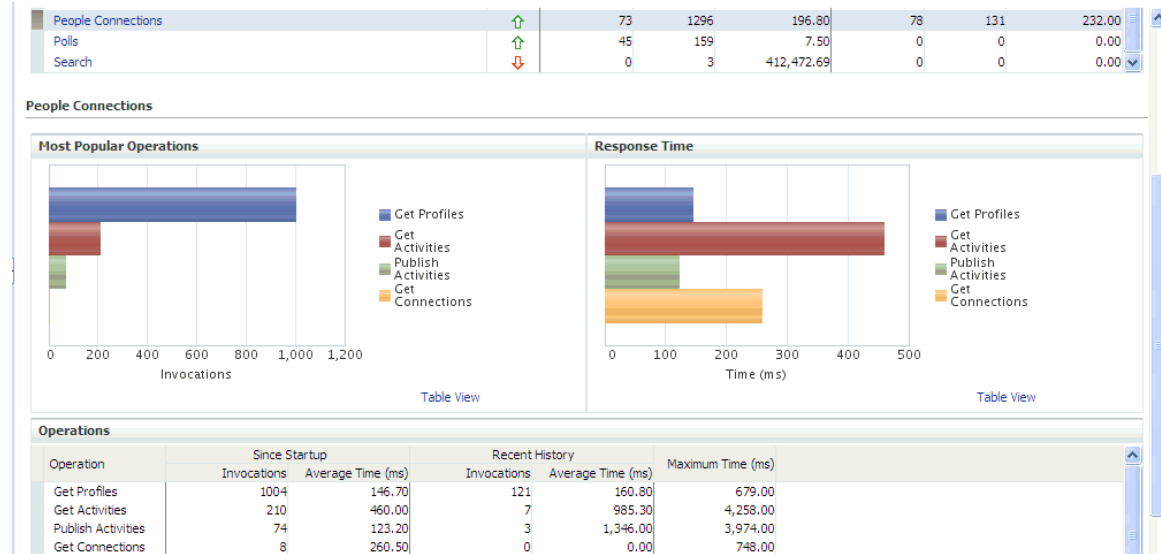
Table 38–23 (Cont.) HTTP Response Codes

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 Portal application-related error, timeout, bad content type response, or SOAP fault.

38.1.4.15 People Connection Metrics

Performance metrics associated with the People Connections service are described in [Table 38–24](#) and [Section 38.1.2, "Common WebCenter Portal Metrics."](#)

Figure 38–17 People Connection Metrics



To monitor these metrics through Fusion Middleware Control, see [Section 38.2, "Viewing Performance Information."](#)

Table 38–24 People Connections Service - Operations Monitored

Operation	Description	Performance Issues - User Action
Get Profiles	Retrieves profiles of a user.	For service-specific causes, see Section 38.1.5.14, "People Connections Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Get Activities	Retrieves the activities based on the user filter options.	For service-specific causes, see Section 38.1.5.14, "People Connections Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."

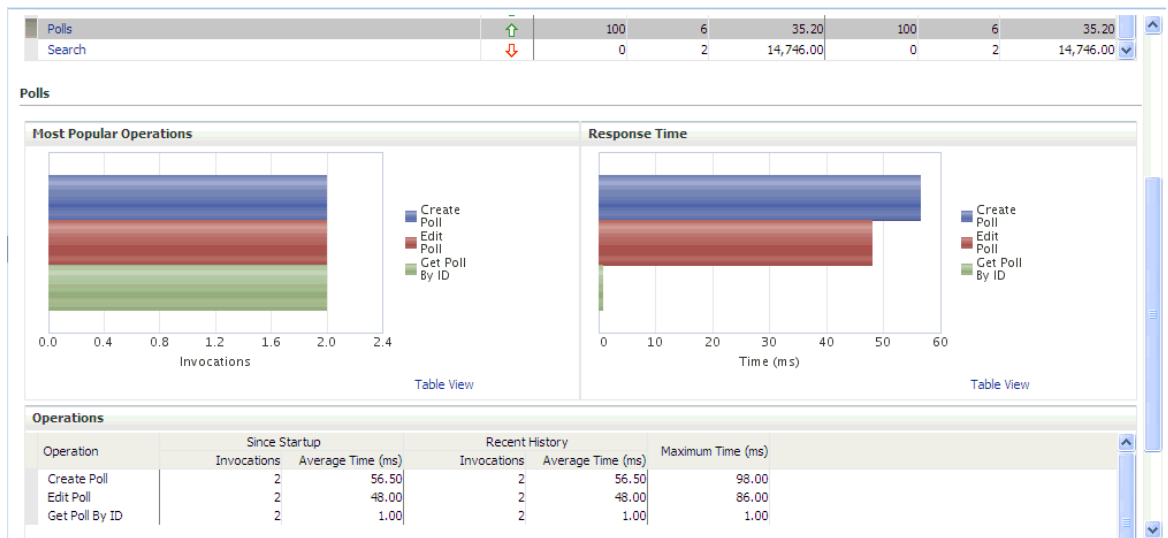
Table 38–24 (Cont.) People Connections Service - Operations Monitored

Operation	Description	Performance Issues - User Action
Publish Activities	Publishes an activity in the user session and saves it in the WebCenter Portal application.	For service-specific causes, see Section 38.1.5.14, "People Connections Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Get Messages	Retrieves the messages of the user.	For service-specific causes, see Section 38.1.5.14, "People Connections Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Get Feedback	Retrieves the feedback of the user.	For service-specific causes, see Section 38.1.5.14, "People Connections Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Get Connections	Retrieves the connections of users.	For service-specific causes, see Section 38.1.5.14, "People Connections Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."

38.1.4.16 Poll Metrics

Performance metrics associated with the Polls service ([Figure 38–18](#)) are described in [Table 38–25](#) and [Section 38.1.2, "Common WebCenter Portal Metrics."](#)

Figure 38–18 Poll Metrics



To monitor these metrics through Fusion Middleware Control, see [Section 38.2, "Viewing Performance Information."](#)

Table 38–25 Polls Service - Operations Monitored

Operation	Description	Performance Issues - User Action
Create Poll	Creates a poll in the WebCenter Portal application.	For service-specific causes, see Section 38.1.5.15, "Polls Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Edit Poll	Edit a poll in the WebCenter Portal application.	For service-specific causes, see Section 38.1.5.15, "Polls Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Delete Poll	Deletes the ongoing poll.	For service-specific causes, see Section 38.1.5.15, "Polls Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Get Poll By ID	Displays the ongoing poll.	For service-specific causes, see Section 38.1.5.15, "Polls Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Submit Poll	Submits the ongoing poll.	For service-specific causes, see Section 38.1.5.15, "Polls Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."
Analyze Results	Analyzes the poll result.	For service-specific causes, see Section 38.1.5.15, "Polls Service." For common causes, see Section 38.1.3, "Common WebCenter Portal Performance Issues and Actions."

38.1.4.17 RSS News Feed Metrics

Performance metrics associated with the RSS service ([Figure 38–19](#)) are described in [Section 38.1.2, "Common WebCenter Portal Metrics."](#)

Figure 38–19 RSS News Feed Metrics

The screenshot shows two tables. The top table is 'Services Summary' and the bottom table is 'RSS News Feeds'.

Service Name	Status	Since Startup		Recent History	
		Successful Invocations (%)	Average Time (ms)	Successful Invocations (%)	Average Time (ms)
Notes	↑	100	35.10	0	0.00
Pages	↑	100	3,125.60	100	115.50
Portlet Producers	↑	99	582.40	100	644.20
Portlets	↑	99	582.40	100	644.20
RSS News Feeds	↑	100	348.40	100	182.00
Recent Activity	↑	100	2,182.70	100	2,182.70
Search	↑	65	382.10	61	48.30

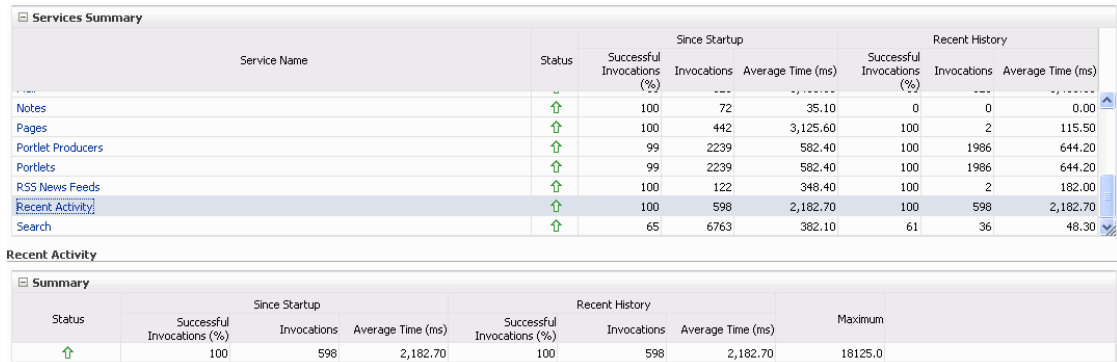
Status	Since Startup			Recent History		
	Successful Invocations (%)	Invocations	Average Page Processing Time (ms)	Successful Invocations (%)	Invocations	Average Page Processing Time (ms)
↑	100	122	348.40	0	0	0.00

To monitor these metrics through Fusion Middleware Control, see [Section 38.2, "Viewing Performance Information."](#)

38.1.4.18 Recent Activity Metrics

Performance metrics associated with the Recent Activities service ([Figure 38–20](#)) are described in [Section 38.1.2, "Common WebCenter Portal Metrics."](#)

Figure 38–20 Recent Activity Metrics

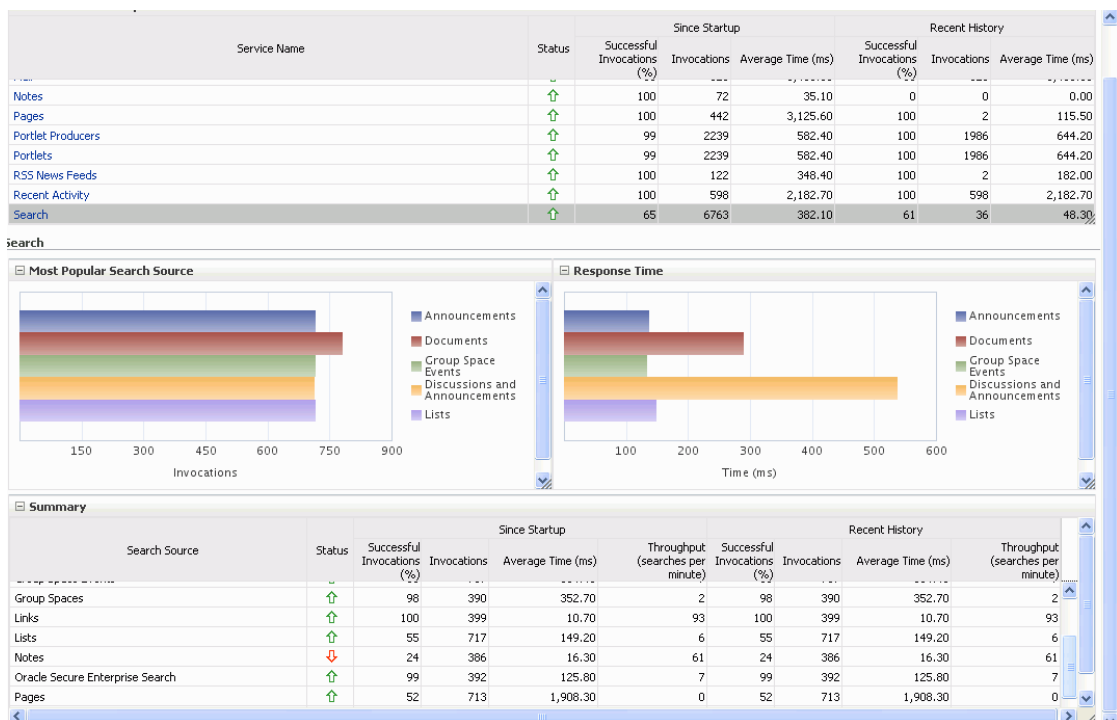


To monitor these metrics through Fusion Middleware Control, see [Section 38.2, "Viewing Performance Information."](#)

38.1.4.19 Search Metrics

Performance metrics associated with the Search service ([Figure 38–21](#)) are described in [Table 38–26](#) and [Section 38.1.2, "Common WebCenter Portal Metrics."](#)

Figure 38–21 Search Metrics



To monitor these metrics through Fusion Middleware Control, see [Section 38.2, "Viewing Performance Information."](#)

Table 38–26 Search Service - Search Sources

Operation	Description
Announcements	Announcement text is searched.
Documents	Contents in files and folders are searched.
Discussion Forums	Forums and topics are searched.
Spaces	Contents saved in a space, such as links, lists, notes, tags, and events are searched.
Space Events	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 Portal services are searched.
Pages	Contents added to application, personal, public, wiki, and blog pages are searched.

38.1.5 WebCenter Portal 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 tuning the performance of WebCenter Portal services, see [Appendix A, "WebCenter Portal Configuration."](#)

- [Section 38.1.5.1, "Announcements Service"](#)
- [Section 38.1.5.2, "BPEL Worklist Service"](#)
- [Section 38.1.5.3, "Content Repository \(Documents and Content Presenter\) Service"](#)
- [Section 38.1.5.4, "Discussions Service"](#)
- [Section 38.1.5.5, "External Applications Service"](#)
- [Section 38.1.5.6, "Events Service"](#)
- [Section 38.1.5.7, "Instant Messaging and Presence \(IMP\) Service"](#)
- [Section 38.1.5.8, "Import and Export"](#)
- [Section 38.1.5.9, "Lists Service"](#)
- [Section 38.1.5.10, "Mail Service"](#)
- [Section 38.1.5.11, "Notes Service"](#)
- [Section 38.1.5.12, "Page Service"](#)
- [Section 38.1.5.13, "Portlets and Producers"](#)
- [Section 38.1.5.14, "People Connections Service"](#)

- [Section 38.1.5.15, "Polls Service"](#)
- [Section 38.1.5.16, "RSS Service"](#)
- [Section 38.1.5.17, "Recent Activities Service"](#)
- [Section 38.1.5.18, "Search Service"](#)

38.1.5.1 Announcements Service

If you are experiencing 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:

- Discussions server is down or not responding.
- Network connectivity issues exist between the application and the Discussions server.
- Connection configuration information associated with the Announcements service is incorrect or no longer valid.

38.1.5.2 BPEL Worklist Service

If you are experiencing 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.

38.1.5.3 Content Repository (Documents and Content Presenter) Service

If you are experiencing 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 WebCenter Content: Content Server (Content Server) and Oracle Portal, verify that the back-end server is up and running.
- For 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 Content Server, go to 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`.

38.1.5.4 Discussions Service

If you are experiencing 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:

- Discussions server is down or not responding.

- Network connectivity issues exist between the application and the discussion server.
- Connection configuration information associated with the Discussions service is incorrect or no longer valid.

38.1.5.5 External Applications Service

If you are experiencing 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 Oracle Internet Directory, is down or not responding.

38.1.5.6 Events Service

If you are experiencing problems with the Events (space events or personal 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 Portal's repository is not available (the database where event information is stored).
- Network connectivity issues exist between the application and the WebCenter Portal's repository.
- Connection configuration information associated with the Events service is incorrect or no longer valid.

38.1.5.7 Instant Messaging and Presence (IMP) Service

If you are experiencing 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.

38.1.5.8 Import and Export

If you are experiencing import and export problems and the status is **Down**, check the diagnostic logs to establish why this service is unavailable.

38.1.5.9 Lists Service

If you are experiencing 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 Portal's 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.

38.1.5.10 Mail Service

If you are experiencing 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.

38.1.5.11 Notes Service

If you are experiencing problems with the Notes service, check if the MDS repository is unavailable or responding slowly (the repository where note information is stored).

38.1.5.12 Page Service

If you are experiencing 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 Portal's repository is not available (the database where page information is stored).
- Network connectivity issues exist between the application and the WebCenter Portal's repository.

38.1.5.13 Portlets and Producers

If you are experiencing 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.

38.1.5.14 People Connections Service

If you are experiencing problems with the People Connections service and the status is **Down**, check the diagnostic logs to establish why this service is unavailable. Some typical causes of failure include:

- The service is down or not responding.
- Connection configuration information associated with the service is incorrect or no longer valid.
- WebCenter Portal's repository is not available (the database where page information is stored).

- Network connectivity issues exist between the application and the WebCenter Portal's repository.

38.1.5.15 Polls Service

If you are experiencing problems with the Polls service and the status is **Down**, check the diagnostic logs to establish why this service is unavailable. Some typical causes of failure include:

- The service is down or not responding.
- Connection configuration information associated with the service is incorrect or no longer valid.
- WebCenter Portal's repository is not available (the database where page information is stored).
- Network connectivity issues exist between the application and the WebCenter Portal's repository.

38.1.5.16 RSS Service

If you are experiencing problems with the RSS 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.

38.1.5.17 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

38.1.5.18 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:

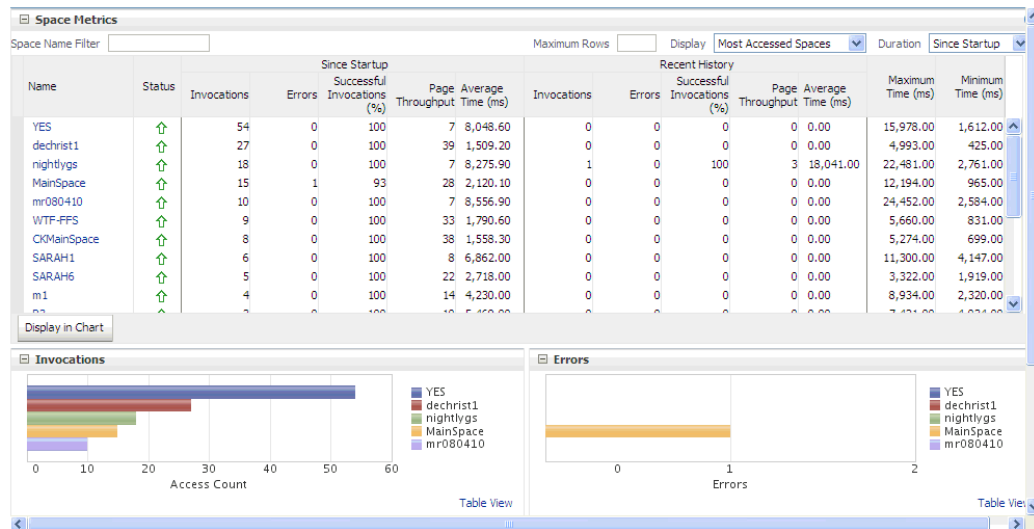
- The repository of the executor is not available.
- Network connectivity issues exist between the application and the repository of the executor.

- Connection configuration information associated with the executor is incorrect or no longer valid.
- Content repositories being searched is currently unavailable.

38.1.6 Space Metrics

(WebCenter Portal: Spaces only) Performance metrics associated with the space activity (Figure 38–22) are described in Table 38–27 and Section 38.1.2, "Common WebCenter Portal Metrics."

Figure 38–22 Space Metrics



To monitor these metrics through Fusion Middleware Control, see Section 38.2, "Viewing Performance Information."

You can filter the data in the following ways:

- Search for a specific space through the **Space Name Filter** field. (Does not show metrics for Home spaces.)
- Display a specific number of rows through the **Maximum Rows** field.
- Display most accessed, least performant, or pages that have maximum errors, through the **Display** dropdown list.

Table 38–27 Space Metrics

Metric	Description
Oracle WebCenter Portal: Spaces URL	The Spaces application being managed.
WebLogic Server	The WebLogic Server instance in which the Spaces application is deployed.
J2EE Application	The name of the Spaces application.
Page Response	The current average response time (in milliseconds) of space pages.

Table 38–27 (Cont.) Space Metrics

Metric	Description
Most Active Spaces	Graph showing the most active spaces, that is, spaces recording the most invocations. To compare a different set of spaces, select one or more spaces in the table, and then click Display in Chart .
Page Throughput	Graph showing the average number of pages processed per minute for each space. To compare a different set of spaces, select one or more spaces in the table, and then click Display in Chart .
Average Processing Time	Graph showing the average page processing time (in milliseconds) per space. To compare a different set of spaces, select one or more spaces in the table, and then click Display in Chart .
Status	The current status of each space: <ul style="list-style-type: none"> ■ Up (Green Up Arrow) - Indicates that the last space operation was successful. The space is up and running. ■ Down (Red Down Arrow) - Indicates that the space is not currently available or the last 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".
Successful Invocations (%)	The percentage of space invocations that succeeded: <ul style="list-style-type: none"> - Since Startup - Recent History <p>If Successful Invocations (%) is below 100%, check the diagnostic logs to establish why service requests are failing. See, Section 38.3, "Viewing and Configuring Log Information."</p>
Invocations	The number of space invocations per minute: <ul style="list-style-type: none"> - Since Startup - Recent History
Errors	The number of errors occurred in a space per minute.
Page Throughput	The average number of pages processed per minute for each space: <ul style="list-style-type: none"> - Since Startup - Recent History
Average Time (ms)	The average time (in ms) to display space pages: <ul style="list-style-type: none"> - Since Startup - Recent History
Maximum Time (ms)	The maximum time taken to display a space page.
Minimum Time (ms)	The minimum time taken to display a space page.

38.1.7 Page Metrics

Performance metrics associated with the page activity ([Figure 38–24](#)) are described in [Table 38–28](#). You can display page metrics for both full and partial pages associated with Spaces applications and Framework applications.

Full Page and Partial Page Metrics

Full page metrics do not include partial page metrics. Partial page rendering of a component on a page increases only partial page metrics and does not cause any change in full page metrics. For example, a calendar refresh on a page increases partial page invocations by 1, but full page invocations remain unchanged.

Partial page requests render only portions of the page. Therefore, you can monitor the performance of pages within a page. Partial page refresh behavior is called partial page rendering (PPR). PPR allows only certain components on a page to be rerendered without the need to refresh the entire page. A common scenario is when an output component displays what a user has chosen or entered in an input component. Similarly, a command link or button can cause another component on the page to be rerendered without refreshing the entire page. For example, if a user takes a quick poll and clicks the Vote button, only the quick poll component is updated and rendered. Hence the full page invocations remain unchanged and the partial page invocations go up by 2. For more information about PPR, see the chapter "Rerendering Partial Page Content" in the *Oracle Fusion Middleware Web User Interface Developer's Guide for Oracle Application Development Framework*.

Note: The page metrics discussed in this section are different from the Page service metrics discussed in [Section 38.1.4.12, "Page Metrics."](#) The Page service metrics, which show up as service metrics, monitor individual operations like creating pages. The Page metrics for spaces, which are discussed in this section, monitor the individual page performance when they are accessed. The Page metrics capture only view/display operations (do not include page edit operations).

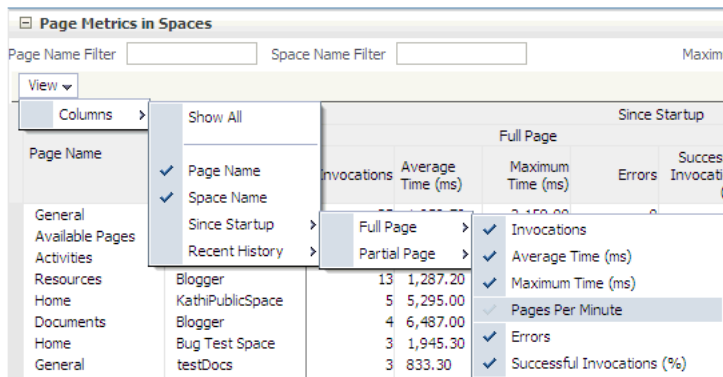
Metrics Display for Pages

You can filter the data in the following ways:

- Search for a specific page through the **Page Name Filter** field.
- Search for a specific space through the **Space Name Filter** field. (relevant only to Spaces applications)
- Display a specific number of rows through the **Maximum Rows** field.
- Display most accessed, least performant, or pages that have maximum errors, through the **Display** dropdown list.

By default the **Pages Per Minute** for full page metrics is hidden. To show this metric, go to the View menu > **Columns** > **Since Startup/Recent History** > **Full Page** > **Pages Per Minute** ([Figure 38–23](#)). Similarly, to hide columns that are not required, deselect the column names.

Figure 38–23 Pages Per Minute Option in the View Menu



Metrics are shown only for custom pages. The metrics for the following types of pages are not shown:

- All pages from any space named *Home space*
- Welcome page of a space
- Service pages such as documents and events

Figure 38–24 Page Metrics in Spaces

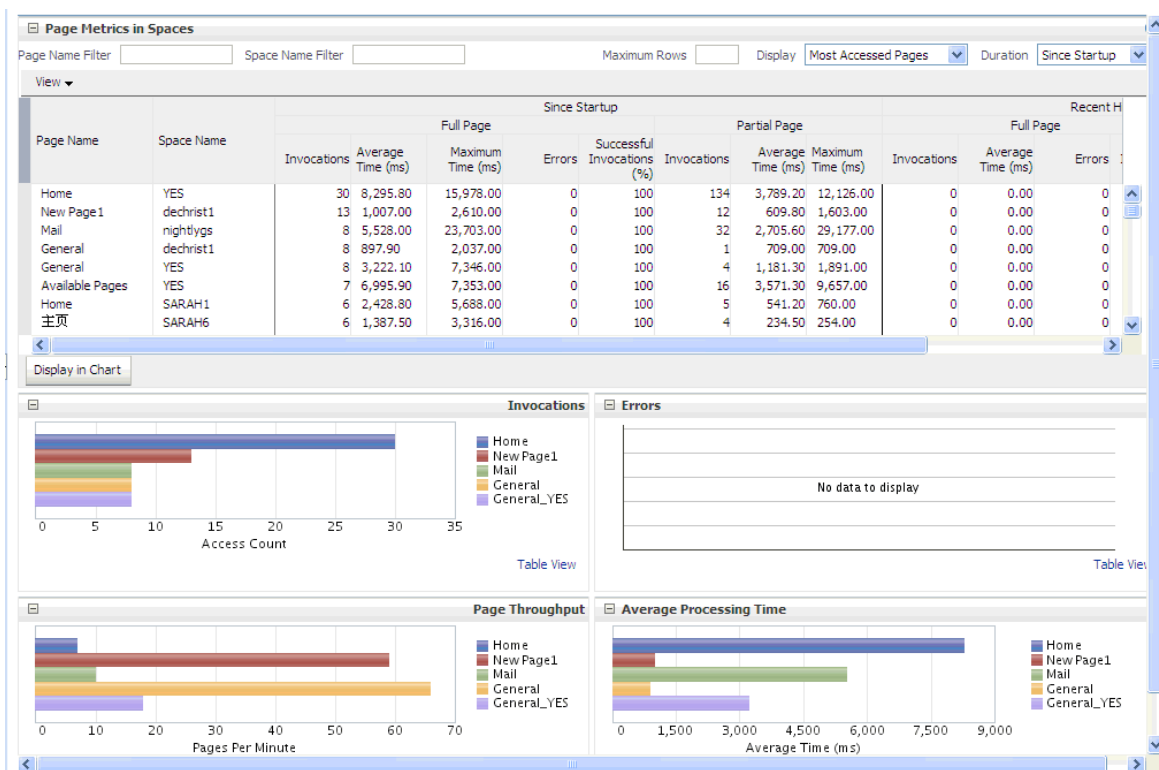


Table 38–28 Page Metrics - Full Page and Partial Page

Metric	Description
Invocations	The number of page invocations per minute: - Since Startup - Recent History

Table 38–28 (Cont.) Page Metrics - Full Page and Partial Page

Metric	Description
Average Time (ms)	The average time (in ms) to display pages: - Since Startup - Recent History
Maximum Time (ms)	The maximum time taken to display a page.
Errors (Only for full page)	The number of errors occurred in a page per minute.
Successful Invocations (Only for full page)	The percentage of page invocations that succeeded: - Since Startup - Recent History If Successful Invocations (%) is below 100%, check the diagnostic logs to establish why service requests are failing. See, Section 38.3, "Viewing and Configuring Log Information."

38.2 Viewing Performance Information

Fusion Middleware Control monitors a wide range of performance metrics for WebCenter Portal applications. You can view performance data for all the dependent services, external applications, and portlet producers used by your WebCenter Portal application.

This section includes the following subsections:

- [Section 38.2.1, "Monitoring a Spaces Applications"](#)
- [Section 38.2.2, "Monitoring Framework Applications"](#)

38.2.1 Monitoring a Spaces Applications

Administrators can monitor the performance and availability of all the components and services that make up a Spaces application, and 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 Spaces home page. You can see at a glance which spaces are the most popular, identify the best and worst performing spaces and more. For details, see [Section 38.1.6, "Space Metrics"](#).

The 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 38.1, "Understanding Oracle WebCenter Portal Performance Metrics."](#)

This section includes the following subsections:

- [Section 38.2.1.1, "Monitoring Service Metrics"](#)
- [Section 38.2.1.2, "Monitoring Space Metrics"](#)
- [Section 38.2.1.3, "Monitoring Page Metrics for the Spaces Application"](#)
- [Section 38.2.1.4, "Monitoring All Metrics Through the Metrics Palette"](#)

38.2.1.1 Monitoring Service Metrics

To access service metrics for the Spaces application:

1. In Fusion Middleware Control Console, navigate to the home page for the Spaces application.

See [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#).

2. From the **WebCenter Portal** menu, choose **Monitoring > Service Metrics**.

Use **Services Summary** at the top of the **WebCenter Portal Service Metrics** page to quickly see which services are up and running, and to review individual and relative performances of those services used by Spaces 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 **Summary** table.

3. Click the name of a service to drill down to more detailed metrics.

To learn more about individual metrics, see [Section 38.1, "Understanding Oracle WebCenter Portal Performance Metrics"](#).

38.2.1.2 Monitoring Space Metrics

To access performance metrics for spaces created in the Spaces application:

1. In Fusion Middleware Control Console, navigate to the home page for Spaces application.

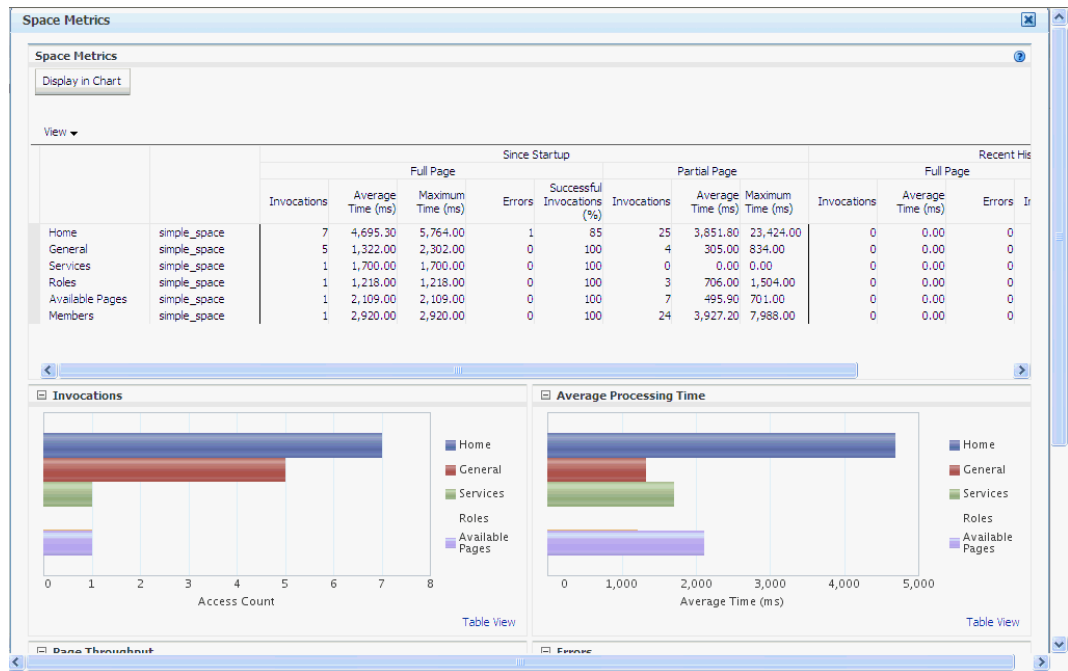
See [Section 6.2, "Navigating to the Home Page for the Spaces Application."](#)

2. From the **WebCenter Portal** menu, choose **Monitoring > Space Metrics**.

3. In the **Space Name Filter** field, enter the name of a space, then press the **[Enter]** key. For information about the space filtering options, see [Section 38.1.6, "Space Metrics."](#)

OR

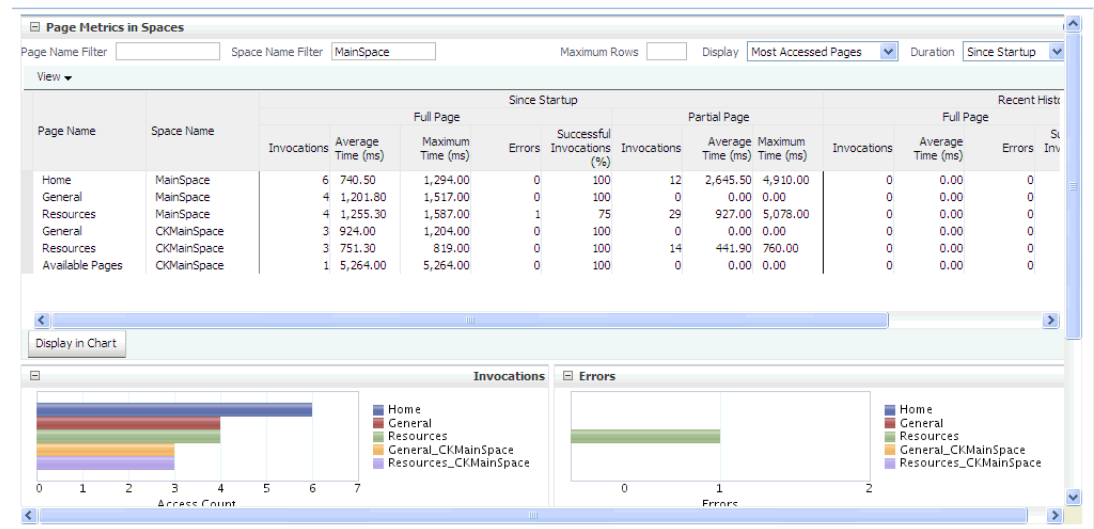
In the **Name** column, click the space name (link) for which you want to display performance metrics. The metrics for the selected space display, as shown in [Figure 38–25](#).

Figure 38–25 Metrics for a Space

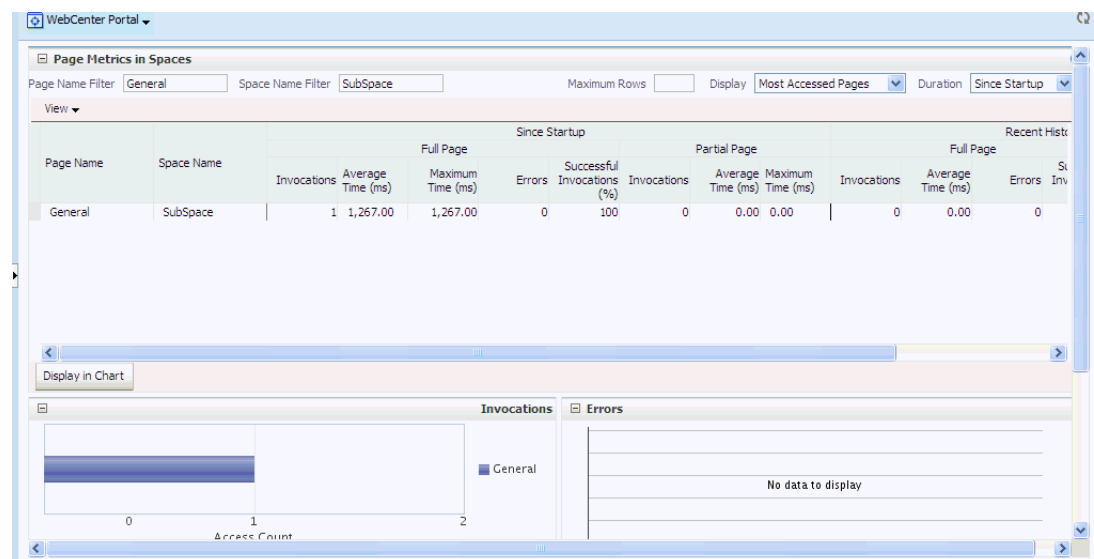
38.2.1.3 Monitoring Page Metrics for the Spaces Application

To access the page metrics:

1. In Fusion Middleware Control Console, navigate to the home page for the Spaces application.
See [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#).
2. From the **WebCenter Portal** menu, choose **Monitoring > Page Metrics**.
For information about available page filtering options, see [Section 38.1.7, "Page Metrics."](#)
3. To see metrics for all pages in a space, enter the name of the space in the **Space Name Filter** field and press **[Enter]**. See [Figure 38–26](#).

Figure 38–26 Page Metrics

- To see metrics for a particular page of a space, enter the page name in the **Page Name Filter** field and the name of the space to which this page belongs, in the **Space Name Filter** field, and then press **[Enter]**. See [Figure 38–27](#).

Figure 38–27 Space Metrics

38.2.1.4 Monitoring All Metrics Through the Metrics Palette

To access performance summary for space and associated pages in the Spaces application:

- In Fusion Middleware Control Console, navigate to the home page for the Spaces application.
See [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#).
- From the **WebCenter Portal** menu, choose **Monitoring > Performance Summary**.

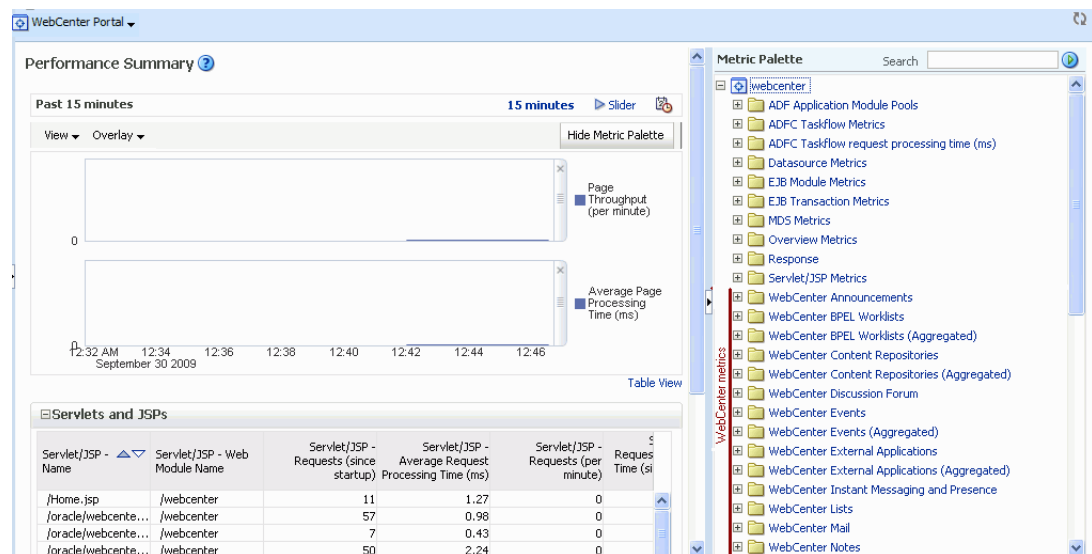
Use the **Show Metric Palette** button at the top of the **Performance Summary** page to display the **Metric Palette**. This palette enables you to select metrics for services that are up and running, and to review live performances of individual services in graphical and tabular formats.

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.

[Figure 38–28](#) shows the Performance Summary page and Metric Palette. In addition to WebCenter Portal performance metrics, the Metric Palette also displays general performance metrics associated with any J2EE application, for example, ADF Application Pool metrics. To display the help content for any metric, right-click the required directory or any metric in the directory and select **Help**.

Figure 38–28 WebCenter Portal: Spaces - Performance Summary and Metric Palette



38.2.2 Monitoring Framework Applications

Administrators can monitor the performance and availability of all the components and services that make up Framework applications, and 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.

This section includes the following subsections:

- [Section 38.2.2.1, "Monitoring Service Metrics"](#)
- [Section 38.2.2.2, "Monitoring Page Metrics for Framework Applications"](#)
- [Section 38.2.2.3, "Monitoring All Metrics Through the Metrics Palette"](#)

38.2.2.1 Monitoring Service Metrics

To access performance metrics for a service associated with a Framework application:

1. In Fusion Middleware Control Console, navigate to the home page for Framework applications.

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

2. From the **Application Deployment** menu, choose **WebCenter Portal > 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 Framework 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 ([Figure 38–28](#)). To display the help content for any metric, right-click the required directory or any metric in the directory and select **Help**.

To learn more about individual metrics for each service, see [Section 38.1, "Understanding Oracle WebCenter Portal Performance Metrics"](#).

38.2.2.2 Monitoring Page Metrics for Framework Applications

To access performance metrics for a page associated with a Framework application:

1. In Fusion Middleware Control Console, navigate to the home page for Framework applications.

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

2. From the **Application Deployment** menu, choose **WebCenter Portal > Page Metrics**.

For information about available page filtering options, see [Section 38.1.7, "Page Metrics."](#)

3. To see metrics for a page, enter the page name in the **Page Name Filter** field and press **[Enter]**.

38.2.2.3 Monitoring All Metrics Through the Metrics Palette

To access service and page performance summary for a Framework application:

1. In Fusion Middleware Control Console, navigate to the home page for Framework applications.

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

2. From the **Application Deployment** menu, choose **Performance Summary**.

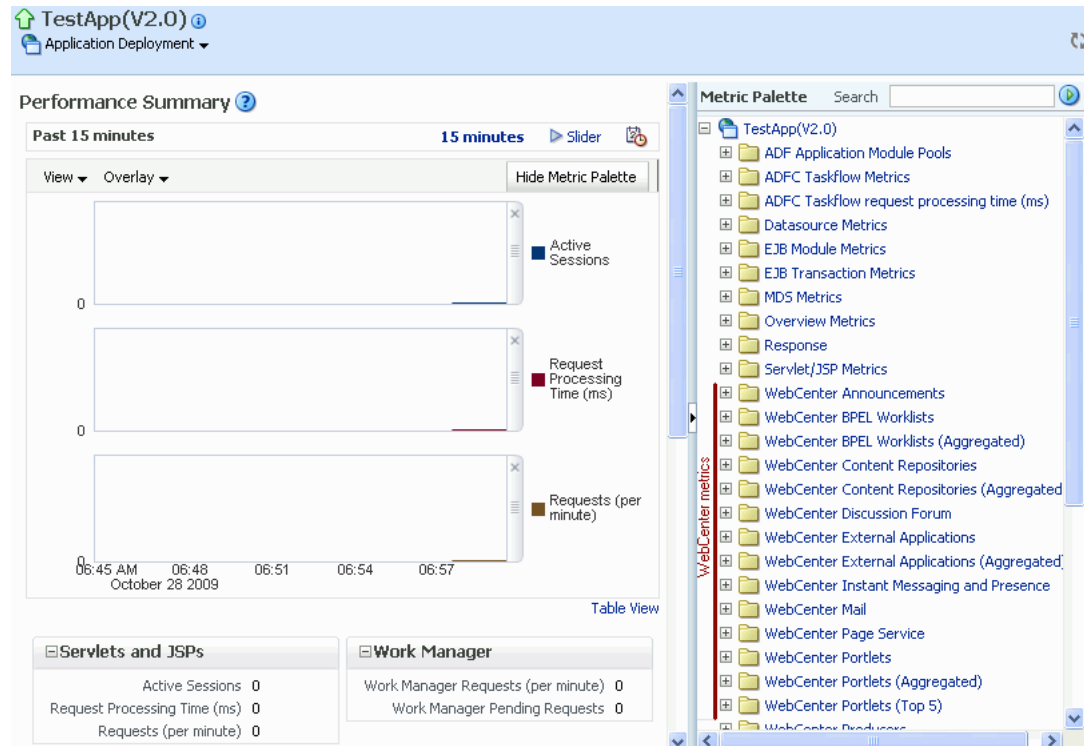
Use the **Show Metric Palette** button at the top of the **Performance Summary** page to display the **Metric Palette**. This palette enables you to select metrics for services that are up and running, and to review live performances of individual services in graphical and tabular formats.

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.

Figure 38–29 shows the Performance Summary page and Metric Palette. In addition to WebCenter Portal performance metrics, the Metric Palette also displays general performance metrics associated with any J2EE application, for example, ADF Application Pool metrics. To display the help content for any metric, right-click the required directory or any metric in the directory and select **Help**.

Figure 38–29 WebCenter Portal: Framework Application - Performance Summary and Metric Palette



38.3 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 Spaces applications, the log file, `WC_Spaces-diagnostic.log` is stored in the `DOMAIN_HOME/servers/WC_Spaces/logs` directory.

For Framework applications, the log file is available in the `DOMAIN_HOME/servers/ServerName/logs` directory. The log file follows the naming convention of `ServerName-diagnostic.log`.

For example, for a managed server, `WC_Custom`, the logs will be stored in the `DOMAIN_HOME/servers/WC_Custom/logs`, and the log file name will be `WC_Custom-diagnostic.log`.

This section includes the following sub sections:

- [Section 38.3.1, "Spaces Application Logs"](#)

- [Section 38.3.2, "Framework Application Logs"](#)

38.3.1 Spaces Application Logs

To view log messages for a Spaces application:

1. In Fusion Middleware Control Console, navigate to the home page for the Spaces application.

See [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#).

2. From the **WebCenter Portal** menu, choose **Logs > View Log Messages**.
3. In the **Log Messages** page, search for warnings, errors, notifications, and so on.

To configure log files for Spaces:

1. In Fusion Middleware Control Console, navigate to the home page for the Spaces application.

See [Section 6.2, "Navigating to the Home Page for the Spaces Application"](#).

2. From the **WebCenter Portal** 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*.

38.3.2 Framework Application Logs

To view log messages for Framework applications:

1. In Fusion Middleware Control Console, navigate to the home page for the Framework application.

See [Section 6.3, "Navigating to the Home Page for Framework 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 for Framework applications:

1. In Fusion Middleware Control Console, navigate to the home page for the Framework application.

See [Section 6.3, "Navigating to the Home Page for Framework 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 Portal

Oracle WebCenter Portal stores data related to its configuration and content for the various feature areas in several locations. To facilitate disaster recovery and the full production lifecycle from development through staging and production, WebCenter Portal provides a set of utilities that enable you to back up this data, move the data between WebCenter Portal applications in staging and production environments. This chapter describes the backup, import, and export capabilities and tools available. It includes the following sections:

- [Section 39.1, "Exporting and Importing a Spaces Application for Data Migration"](#)
- [Section 39.2, "Exporting and Importing Framework Applications for Data Migration"](#)
- [Section 39.3, "Migrating Wiki Documents from Other Wiki Applications"](#)
- [Section 39.4, "Backing Up and Recovering WebCenter Portal Applications"](#)
- [Section 39.5, "Troubleshooting Import and Export Issues for Spaces"](#)

To best plan the proper usage of these tools, record which WebCenter Portal features your WebCenter Portal applications are using: Spaces, Framework, Discussion server, Oracle WebCenter Content Server, and so on.

Note: If you want to migrate a test instance to a production instance, refer to "Moving Oracle WebCenter Portal from a Test to Production Environment" in *Oracle Fusion Middleware Administrator's Guide*. This section describes an alternative approach to the steps described in this chapter (some of the steps are automated).

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"](#).

39.1 Exporting and Importing a Spaces Application for Data Migration

Spaces provides a set of export and import utilities that enable you to back up or move content between Spaces applications and stage or production environments. This section describes how to export and import the whole Spaces application, and also individual spaces and space templates. It includes the following subsections:

- [Section 39.1.1, "Understanding Spaces Export and Import"](#)

- [Section 39.1.2, "Prerequisites for Spaces Application Export and Import"](#)

Migrating an entire Spaces application:

- [Section 39.1.3, "Migrating Back-end Components for an Entire Spaces Application"](#)
- [Section 39.1.4, "Exporting an Entire Spaces Application"](#)
- [Section 39.1.5, "Importing an Entire Spaces Application"](#)

Migrating individual spaces:

- [Section 39.1.6, "Prerequisites for Individual Space Export and Import"](#)
- [Section 39.1.7, "Migrating Back-end Components for Individual Spaces"](#)
- [Section 39.1.8, "Exporting Individual Spaces"](#)
- [Section 39.1.9, "Importing Individual Spaces"](#)

Migrating space templates:

- [Section 39.1.10, "Migrating Back-end Components for Space Templates"](#)
- [Section 39.1.11, "Exporting Space Templates"](#)
- [Section 39.1.12, "Importing Space Templates"](#)

Migrating Spaces resources:

- [Section 39.1.13, "Exporting Spaces Resources"](#)
- [Section 39.1.14, "Importing Space Resources"](#)

39.1.1 Understanding Spaces Export and Import

Using export and import, Fusion Middleware administrators can migrate entire Spaces applications between stage and production environments. This includes every space, space template, user-defined resources, customizations (applied to the application, pages, and task flows), application and service metadata (object definitions), and other data, as outlined in [Figure 39-1](#).

Figure 39–1 Information Exported with a Spaces Application

Always Exported	Export Optional	Never Exported
MDS – Service Metadata <ul style="list-style-type: none"> • Announcements • Discussions • Documents • Events • Lists (Definitions) • Notes • Mail • Pages • Portlets • Recent Activities • Resource Catalog • RSS News Feeds • Search • Tags • Worklists MDS – Service Data <ul style="list-style-type: none"> • Notes MDS – Service Customizations <ul style="list-style-type: none"> • Portlets • Pages WebCenter Resources <ul style="list-style-type: none"> • Page Templates • Navigations • ResourceCatalogs • Skins • Page Styles • Content Templates • Mashup Styles • Data Controls • Task Flows Application Artifacts (in the Content Directory) <ul style="list-style-type: none"> • Icons • Images... Security Policy <ul style="list-style-type: none"> • policy-store.xml: <ul style="list-style-type: none"> ◦ Application roles and permissions ◦ Space roles and permissions • User role assignments 	MDS – Task Flow Customizations <ul style="list-style-type: none"> • Documents: <ul style="list-style-type: none"> - Content Presenter - Document Library - Document List Viewer • Events - Events • Lists - List Viewer • Polls - Quick Poll <ul style="list-style-type: none"> - Polls Manager - Take Polls - View Poll Results • Search - Saved Searches MDS – Application Customizations <ul style="list-style-type: none"> • WebCenter Spaces: <ul style="list-style-type: none"> ◦ WebCenter Administration* <ul style="list-style-type: none"> - System Pages ◦ Space Administration <ul style="list-style-type: none"> - Space-level Resources MDS – Resource Customizations <ul style="list-style-type: none"> • Page Templates WebCenter Repository – Service Data <ul style="list-style-type: none"> • Space Events • Links • Lists • Tags • Polls • People Connections: <ul style="list-style-type: none"> ◦ Default Settings for Profiles, Message Boards, Feedback, Connections, Activity Streams ◦ Activity Stream Task Flow Customizations 	MDS – User Customizations <ul style="list-style-type: none"> • Pages • Task Flows** • Application External – Service Data <ul style="list-style-type: none"> • Documents • Wikis and Blogs • Activity Graph • Analytics • Announcements • Discussions • IMP • Mail • Personal Events • Worklists Application Artifacts (not in the Content Directory) <ul style="list-style-type: none"> • Icons • Images...

* Except for People Connection Settings

** Except for Activity Stream Task Flow Customizations

This migration can be performed using Fusion Middleware Control or WLST commands. For details, see:

- [Section 39.1.4.1, "Exporting the Spaces Application Using Fusion Middleware Control"](#)
- [Section 39.1.4.2, "Exporting the Spaces Application Using WLST"](#)
- [Section 39.1.5.1, "Importing a Spaces Application Using Fusion Middleware Control"](#)

- [Section 39.1.5.2, "Importing a Spaces Application Using WLST"](#)

Space and Space Template Export and Import

Spaces administrators can also export and import individual spaces and space templates, and their related objects, through Spaces Administration. Several WLST commands for migrating individual spaces and space templates are available too.

The primary purpose of these export and import features is to enable cloning and migration of data. The export and import combination enables Spaces administrators to:

- Move spaces and space templates and related objects stored in Content Server between stage and production environments.
- Move spaces and space templates and related objects stored in Content Server to remote instances.

For more detail, see.

- [Section 39.1.8, "Exporting Individual Spaces"](#)
- [Section 39.1.9, "Importing Individual Spaces"](#)
- [Section 39.1.11, "Exporting Space Templates"](#)
- [Section 39.1.12, "Importing Space Templates"](#)

Application Customizations and User Customizations

Some Spaces application customizations are optional on export, as noted in [Figure 39–1](#). If you want to migrate application-level customizations you must set the export option "Include Customizations". For more information, reference [Table 39–4, "Spaces Services - Application Customizations"](#) and [Table 39–5, "Spaces - Application Customizations"](#) at the end of this chapter.

User-level customizations are not migrated during export and import. For more information on application customization and user customization and the difference between them, see "What You Should Know About Customizing Page Components" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

39.1.2 Prerequisites for Spaces Application Export and Import

The database in which the application metadata or schema is stored must be up and running for the export and import operation to work. If your application contains any Web Service data controls, all the associated Web Services must also be up and accessible for the export and import to succeed.

In addition, Oracle recommends that you migrate all the back-end components *before* you export or import a Spaces application. For more information, refer to the section, [Section 39.1.3, "Migrating Back-end Components for an Entire Spaces Application."](#)

Spaces is temporarily unavailable during import and export operations to prevent data conflicts. Any user who tries to login or access a Spaces page sees an "application unavailable" page.

39.1.3 Migrating Back-end Components for an Entire Spaces Application

Before migrating a Spaces application, you must migrate all the back-end components that are used by the application. This section tells you how to migrate the Identity Store, Credential Store, Policy Store, Discussions Server, Content Server, Oracle WebLogic Communications Server, and portlet producers.

The configured services in the target instance must be a superset of the services that are configured in the source instance. 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 operation fails.

This section includes the following sub-sections:

- [Section 39.1.3.1, "Exporting the LDAP Identity Store"](#)
- [Section 39.1.3.2, "Importing the LDAP Identity Store"](#)
- [Section 39.1.3.3, "Exporting and Importing the LDAP Credential Store"](#)
- [Section 39.1.3.4, "Exporting and Importing the LDAP Policy Store"](#)
- [Section 39.1.3.5, "Exporting and Importing a File-based Credential Store"](#)
- [Section 39.1.3.6, "Exporting and Importing a File-based Policy Store"](#)
- [Section 39.1.3.7, "Exporting Discussions Server Data"](#)
- [Section 39.1.3.8, "Importing Discussions Server Data"](#)
- [Section 39.1.3.9, "Exporting Oracle Content Server Data"](#)
- [Section 39.1.3.10, "Importing Oracle Content Server Data"](#)
- [Section 39.1.3.11, "Exporting Oracle WebLogic Communications Server"](#)
- [Section 39.1.3.12, "Importing Oracle WebLogic Communications Server"](#)
- [Section 39.1.3.13, "Exporting Portlet Producers"](#)
- [Section 39.1.3.14, "Importing Portlet Producers"](#)

39.1.3.1 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 `IDM_ORACLE_HOME/bin` directory.

[Example 39–1](#) shows the `ldapsearch` command for exporting an LDAP identity store. Where `LDAP_OH/bin` is the OID/IdM `IDM_ORACLE_HOME/bin` directory:

Example 39–1 *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
```

When exporting users, ensure that the command includes the `orclguid` attribute, as shown in [Example 39–1](#).

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 Identity Management User Reference*.

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*. Ensure that the command includes the `orclguid` attribute.

The source and target LDAP servers must both be the same type, that is, both embedded LDAP servers or both external LDAP servers. It is not possible, for example, to migrate users, groups, and passwords stored in an embedded LDAP server to an external LDAP server.

39.1.3.2 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 `IDM_ORACLE_HOME/bin` directory.

[Example 39-2](#) shows how to run the `ldapaddmt` utility to import the `ldif` file. Where `LDAP_OH/bin` is the OID/IdM `IDM_ORACLE_HOME/bin` directory:

Example 39-2 *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 Identity Management User Reference*.

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*.

The source and target LDAP servers must both be the same type, that is, both embedded LDAP servers or both external LDAP servers. It is not possible, for example, to migrate users, groups, and passwords stored in an embedded LDAP server to an external LDAP server.

39.1.3.3 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
```

1

- 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 contains 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. You are only concerned with the credential store, therefore, 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 application.

The folder name returned is named: <application_name>-xxxx

For 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=JPContext,
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 application.

The folder name returned is named: <application_name>-xxxx

For Spaces, <application_name> is always webcenter.

4. To import the credential store, run the WLST command migrateSecurityStore.

For example (Example 39-3):

Example 39-3 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*.

39.1.3.4 Exporting and Importing the LDAP Policy Store

With Spaces, there is no need for manual policy store migration because the Spaces export/import commands migrate security policy data for you. For details, see [Section 39.1.4, "Exporting an Entire Spaces Application."](#)

Oracle does not recommend that you perform policy store migration manually for Spaces, but there may be circumstances where this is required. In such cases, use the WLST command migrateSecurityStore to perform the migration as described below.

Note: For other WebCenter Portal 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 contains 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 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 application.

The application name returned is: `<application_name>xxxxx`

For 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 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 application.

The application name returned is: `<application_name>xxxxx`

For Spaces, `<application_name>` is always `webcenter`.

4. To import the policy store, run the WLST command `migrateSecurityStore`.

For example (Example 39-4):

Example 39-4 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*.

39.1.3.5 Exporting and Importing a File-based Credential Store

To migrate a file-based 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 the target's `jps-config.xml` file.

1. Backup your target's `jps-config.xml` file located at `DOMAIN_HOME/config/fmwconfig/jps-config.xml`.
2. Add source and target information to the target's `jps-config.xml`:
 - a. Add the following section (above the closing `</serviceInstances>` tag) to point to the *source* credential store:

```
<serviceInstance name="sourcecredstore" provider="credstoressp"
location="/MW_HOME/user_projects/domains/base-domain/config/fmwconfig/.">
  <description>File Based Credential Store Service
Instance</description>
</serviceInstance>
```

Replace `/MW_HOME/user_projects/domains/base-domain` with the path to the source domain.

- b. Update the credential store reference to point to the value specified in step a. Add the following entries above the closing `</jpsContexts>` tag:

```
<jpsContext name="targetcredstore">
  <serviceInstanceRef ref="credstore"/>
</jpsContext>
<jpsContext name="sourcecredstore">
  <serviceInstanceRef ref="sourcecredstore"/>
</jpsContext>
```

3. Import the file-based credential store using the WLST command `migrateSecurityStore`.

For example (Example 39-5):

Example 39-5 migrateSecurityStore - Credential Store

```
migrateSecurityStore(type="credStore",
configFile="/MW_HOME/user_projects/domains/base-domain/config/fmwconfig/jps-config.xml", src="sourcecredstore", dst="targetcredstore")
```

Note that the `configFile` parameter maps to the `jps-config.xml` file in the target domain, and that the `src` and `dst` parameters map to the newly created `jpsContext` elements.

For detailed syntax and examples, see "migrateSecurityStore" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

Output similar to the following displays and includes a WARNING that you can ignore:

```
{srcFolder=null, preserveAppRoleGuids=null, dst=targetcredstore, type=credStore,
dstFolder=null, resourceTypeFile=null, dstLdifFile=null, srcApp=null,
configFile=/scratch/product/target/user_projects/domains/domain4/config/fmwconfig/
jps-config.xml,
dstApp=null, srcConfigFile=null, src=sourcecredstore, overWrite=null,
migrateIdStoreMapping=null, processPrivRole=null}
Oct 26, 2009 11:23:42 AM
oracle.security.jps.internal.tools.utility.destination.apibased.JpsDstCredential
setCredential
WARNING: Cannot migrate credential folder/key
webcenter-1111/anonymous#oracle.portlet.client.adapter.adf.ADFPortletContainerExte
rnalConfig.Reason
oracle.security.jps.service.credstore.CredentialAlreadyExistsException:
The credential with map webcenter-1111 and key
anonymous#oracle.portlet.client.adapter.adf.ADFPortletContainerExternalConfig
```

already exists.

39.1.3.6 Exporting and Importing a File-based Policy Store

With Spaces, there is no need for manual policy store migration because the Spaces export/import commands migrate security policy data for you. For details, see [Section 39.1.4, "Exporting an Entire Spaces Application."](#)

Oracle does not recommend that you perform policy store migration manually for Spaces but there may be circumstances where this is required. In such cases, use the WLST command `migrateSecurityStore` to perform the migration as described below.

Note: For other WebCenter Portal 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 your target's `jps-config.xml` file.

1. Backup your target's `jps-config.xml` file located at `DOMAIN_HOME/config/fmwconfig/jps-config.xml`.
2. Add source and target information to the target's `jps-config.xml`:
 - a. Add the following section (above the closing `</serviceInstances>` tag) to point to the *source* policy store:

```
<serviceInstance name="srcpolicystore.xml"
  provider="policystore.xml.provider"
  location="/MW_HOME/user_projects/domains/base_domain/config/fmwconfig/system-jazn-data.xml">
  <description>File Based Policy Store Service Instance</description>
</serviceInstance>
```

Replace `/MW_HOME/user_projects/domains/base-domain` with the path to the source domain.

- b. Update the policy store reference to point to the value specified in step a. Add the following entries above the closing `</jpsContexts>` tag:

```
<jpsContext name="targetFileStore">
  <serviceInstanceRef ref="policystore.xml"/>
</jpsContext>
<jpsContext name="sourceFileStore">
  <serviceInstanceRef ref="srcpolicystore.xml"/>
</jpsContext>
```

3. Import the file-based credential store using the WLST command `migrateSecurityStore`.

For example ([Example 39-6](#)):

Example 39-6 migrateSecurityStore - Credential Store

```
migrateSecurityStore(type="appPolicies", srcApp="webcenter",
  configFile="/MW_HOME/user_projects/domains/base_domain/config/fmwconfig/jps-config.xml",
  src="sourceFileStore", dst="targetFileStore", overwrite="true")
```

Note that the `configFile` parameter maps to the `jps-config.xml` file in the target domain, and that the `src` and `dst` parameters map to the newly created `jpsContext` elements.

For detailed syntax and examples, see "migrateSecurityStore" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

Output similar to the following displays and includes a WARNING that you can ignore:

```
{srcFolder=null, dst=targetFileStore,
type=appPolicies, dstFolder=null, resourceTypeFile=null,
dstLdifFile=null, srcApp=webcenter,
configFile=/scratch/product/target/user_projects/domains/base_domain/config/fmwcon
fig/jps-config.xml,
dstApp=null, srcConfigFile=null, src=sourceFileStore, overWrite=true,
migrateIdStoreMapping=null, processPrivRole=null}Oct 26, 2009 4:14:42 AM
oracle.security.jps.internal.tools.utility.destination.apibased.JpsDstPolicy
<init>
WARNING: No identity store associate with policy store found.
wls:/offline>
```

39.1.3.7 Exporting Discussions Server Data

To export WebCenter Portal's discussions server data, use the appropriate database export utility:

- For an Oracle database, go to `ORACLE_HOME/bin` of your database and run the command described in [Example 39-7](#).
- For non-Oracle databases, refer to the manufacturer's documentation.

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, the *Oracle Database Utilities* guide.

Example 39-7 Export Database Utility

```
DB_ORACLE_HOME/bin/expdp \ "sys/password@serviceid as sysdba"
OWNER=srcrcuprefix_DISCUSSIONS DUMPFILE=/tmp/df.dmp STATISTICS=none
```

where:

- `DB_ORACLE_HOME` is the directory in which the database for WebCenter Portal's discussion server schema is installed.
- `password` is the password for the system database user.
- `serviceid` is the service ID of the database connection.
- `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`.
- `DUMPFILE` contains the exported data.

39.1.3.8 Importing Discussions Server Data

To import discussions server data, use the appropriate database import utility:

- For an Oracle database, follow the steps below.

- For non-Oracle databases, refer to the manufacturer's documentation.

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, the *Oracle Database Utilities* guide.

1. Shut down the target discussions server.
2. Go to `DB_ORACLE_HOME/bin` of the database where WebCenter Portal's discussions server schema is installed, and connect to the database using `sqlplus` as `sysdba`:

```
DB_ORACLE_HOME/bin/sqlplus "sys/password@serviceid 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_IAS_DISCUSSIONS temporary tablespace name_IAS_TEMP;
```

where:

- `tgtrcuprefix_DISCUSSIONS` is the user name. This is the RCU suffix that was used during installation, `_DISCUSSIONS`, along with a user supplied prefix. For example, `DEV_DISCUSSIONS`.
 - `password` is the password for the target user.
 - `tgtrcuprefix_IAS_DISCUSSIONS` identifies the default tablespace. For example, the RCU suffix that was used during installation, `IAS_DISCUSSIONS`, along with a user supplied prefix. For example, `DEV_IAS_DISCUSSIONS`.
 - `name_IAS_TEMP` identifies the temporary tablespace. For example, `DEV_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 39-8](#).

Example 39-8 Database Import Utility

```
DB_ORACLE_HOME/bin/impdp "sys/password@serviceid as sysdba"
remap_schema=srcrcuprefix_DISCUSSIONS:tgtrcuprefix_DISCUSSIONS
remap_tablespace=source_tablespace:target_tablespace DUMPFILE=/tmp/df.dmp
STATISTICS=none
```

where:

- `DB_ORACLE_HOME` is the directory in which the database for WebCenter Portal's discussions server schema is installed.
- `password` is the password for the system database user.
- `serviceid` is the service ID of the database connection.

- `REMAP_SCHEMA` identifies the source and target schemas. For example, schema names include the RCU suffix that was used during installation, `_DISCUSSIONS`, along with the user supplied prefix. For example, `DEV_DISCUSSIONS`.
- `REMAP_TABLESPACE` identifies the source and target tablespace. Remaps all objects selected for import with persistent data in the source tablespace to be created in the target tablespace. For example, `source_tablespace:target_tablespace`.
- `DUMPFIL` contains the data to be imported.

39.1.3.9 Exporting Oracle Content Server Data

First use Oracle Data Pump to export the Oracle WebCenter Content Server schema, and then export the native (vault) and web-viewable (weblayout) files.

Note: For non-Oracle databases, refer to the manufacturer's documentation.

1. Export Content Server data using the Oracle Data Pump export utility.

For example, go to `ORACLE_HOME/bin` of your database and run the command described in [Example 39-9](#).

Note: The Oracle Data Pump utility does not support LONG columns types that exist in the OCSEVER schema. Therefore, Oracle recommends using Oracle Database Utilities. See also, the *Oracle Database Utilities* guide.

Example 39-9 Data Pump Utility (Export)

```
DB_ORACLE_HOME/bin/expdp \"sys/password@serviceid as sysdba\"
OWNER=srcrcuprefix_OCSEVER DUMPFIL=/tmp/ucm.dmp STATISTICS=none
```

where:

- `DB_ORACLE_HOME` is the directory in which the database for Oracle WebCenter Content Server schema is installed.
 - `password` is the password for system database user.
 - `serviceid` is the service ID of the database connection.
 - `OWNER` is the schema to be exported. This is the RCU suffix that was used during installation, `_OCSEVER`, along with the user supplied prefix. For example, `DEV_OCSEVER`.
 - `DUMPFIL` contains the exported data.
2. Export the native (vault) and web-viewable (weblayout) files:
 - **Vault files** - Tar up the `<WC_ORACLE_HOME>/ucm/vault` folder on the source system. For example:


```
tar cvf ucm_vault.tar WC_ORACLE_HOME/ucm/vault
```
 - **Weblayout files** - Tar up the `<WC_ORACLE_HOME>/ucm/weblayout` folder on the source system. For example:

```
tar cvf ucm_weblayout.tar WC_ORACLE_HOME/ucm/weblayout
```

3. Import the source `vault` and `weblayout` folder archives on the target system as follows:

- **Vault files** - Restore the `vault` folder. For example:

```
cd WC_ORACLE_HOME/ucm;
tar xvf ucm_vault.tar
```

- **Weblayout files** - Restore the `weblayout` folder. For example:

```
cd WC_ORACLE_HOME/ucm;
tar xvf ucm_weblayout.tar
```

39.1.3.10 Importing Oracle Content Server Data

First use Oracle Data Pump to import the source Oracle WebCenter Content Server schema, and then import the source `vault` and `weblayout` folder archives.

Note: For non-Oracle databases, refer to the manufacturer's documentation.

1. Shut down the target Content Server.
2. Go to `DB_ORACLE_HOME/bin` of the database where Oracle WebCenter Content Server schema is installed, and connect to the database using `sqlplus` as `sysdba`:

```
DB_ORACLE_HOME/bin/sqlplus "sys/password@serviceid as sysdba"
```

3. Drop the target user:

```
drop user tgtrcuprefix_OCSERVER cascade;
```

4. Create the target user:

```
create user tgtrcuprefix_OCSERVER identified by password default tablespace
tgtrcuprefix_OCSERVER temporary tablespace name_IAS_TEMP;
```

where:

- `tgtrcuprefix_OCSERVER` is the user name. This is the RCU suffix that was used during installation, `_OCSERVER`, along with a user supplied prefix. For example, `DEV_OCSERVER`.
- `password` is the password for the target user.
- `tgtrcuprefix_IAS_OCSERVER` identifies the default tablespace. For example, the RCU suffix that was used during installation, `IAS_OCSERVER`, along with a user supplied prefix. For example, `DEV_IAS_OCSERVER`.
- `name_IAS_TEMP` identifies the temporary tablespace. For example, `DEV_IAS_TEMP`.

5. Grant connect and resource to the user:

```
grant connect,resource to tgtrcuprefix_OCSERVER;
```

6. Import Content Server data using the Oracle Data Pump import utility.

For example, in `DB_ORACLE_HOME/bin` of your database, run the command described in [Example 39-10](#).

Note: The Oracle Data Pump utility does not support LONG columns types that exist in the OCSERVER schema. Therefore, Oracle recommends using Oracle Database Utilities. See also, the *Oracle Database Utilities* guide.

Example 39–10 Data Pump Utility (Import)

```
DB_ORACLE_HOME/bin/impdp \ "sys/password@serviceid as sysdba\"
remap_schema=srcrcuprefix_OCSERVER:tgtrcuprefix_OCSERVER
remap_tablespace=source_tablespace:target_tablespace DUMPFILE=/tmp/UCM.dmp
STATISTICS=none TRANSFORM=oid:n
```

where:

- `DB_ORACLE_HOME` is the directory in which the database for the Oracle WebCenter Content Server schema is installed.
 - `password` is the password for system database user.
 - `serviceid` is the service ID of the database connection.
 - `REMAP_SCHEMA` identifies the source and target schemas. For example, schema names include the RCU suffix that was used during installation, `_OCSERVER`, along with the user supplied prefix. For example, `DEV_OCSERVER`.
 - `REMAP_TABLESPACE` identifies the source and target tablespace. Remaps all objects selected for import with persistent data in the source tablespace to be created in the target tablespace. For example, `source_tablespace:target_tablespace`.
 - `DUMPFILE` contains the data to be imported.
7. Import the source `vault` and `weblayout` folder archives on the target system as follows:
- **Vault files** - Restore the `vault` folder. For example:

```
cd WC_ORACLE_HOME/ucm;
tar xvf ucm_vault.tar
```
 - **Weblayout files** - Restore the `weblayout` folder. For example:

```
cd WC_ORACLE_HOME/ucm;
tar xvf ucm_weblayout.tar
```

After importing the Oracle WebCenter Content Server data, log in to the Spaces application and open any imported space. Verify that the Documents service is enabled in that space and that imported folders are available as expected.

39.1.3.11 Exporting Oracle WebLogic Communications Server

For information on exporting Oracle WebLogic Communications Server, see *Oracle WebLogic Communication Services Administrator's Guide*.

39.1.3.12 Importing Oracle WebLogic Communications Server

For information on importing Oracle WebLogic Communications Server, see *Oracle WebLogic Communication Services Administrator's Guide*.

39.1.3.13 Exporting Portlet Producers

This step is only require to migrate entire producer metadata and not just the producer metadata associated with your 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 Portal*.

39.1.3.14 Importing Portlet Producers

This step is only required to migrate entire producer metadata and not just the producer metadata associated with your 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 Portal*.

39.1.4 Exporting an Entire Spaces Application

This section describes how to export an entire Spaces application using Fusion Middleware Control and WLST commands.

A Spaces application is exported into a single export archive (.ear file). The EAR file contains:

- a metadata archive (.mar) file
- an XML file containing security policy information (`policy-store.xml`):
 - application roles (and permissions assigned to each role)
 - users details and their application role assignments in the Home space
 - individual space members (and their role assignments in each space)

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 39.1.1, "Understanding Spaces Export and Import"](#).

The Spaces application is temporarily unavailable during import and export operations to prevent data conflicts. Any user who tries to login or access a Spaces page see an "application unavailable" page.

The export process does not include data associated with external services, that is, Mail, Discussions, Announcements, Worklists, Personal Events, Instant Messaging and Presence (IMP), and Documents. To learn how to move data associated with these services, see [Section 39.1.3, "Migrating Back-end Components for an Entire Spaces Application."](#)

The users in both the export and import environment must be identical. If a shared identity store is not used, then these users must also be migrated. Refer to [Section 39.1.3, "Migrating Back-end Components for an Entire Spaces Application."](#)

Note: Only application artifacts located in the *content directory* are exported. For example, icons and images, and so on, associated with a page template must be placed in the page template's content directory to be exported. For more information, see "What You Should Know About a Resource's Properties" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

Out-of-the-box templates and user customizations are never exported. For more information on user customizations, see the section "What You Should Know About Customizing Page Components" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

This section includes the following:

- [Section 39.1.4.1, "Exporting the Spaces Application Using Fusion Middleware Control"](#)
- [Section 39.1.4.2, "Exporting the Spaces Application Using WLST"](#)

39.1.4.1 Exporting the Spaces Application Using Fusion Middleware Control

Fusion Middleware administrators can export an entire Spaces application using Fusion Middleware Control.

To export Spaces:

1. In Fusion Middleware Control, navigate to the home page for Spaces.
See [Section 6.2, "Navigating to the Home Page for the Spaces Application."](#)
2. From the **WebCenter Portal** menu, select **Application Export**, as shown in [Figure 39–2](#).

Figure 39–2 WebCenter Portal 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 39–3](#).

Figure 39–3 Naming the Export Archive

4. Set export options as required. For details, see [Table 39–1](#).

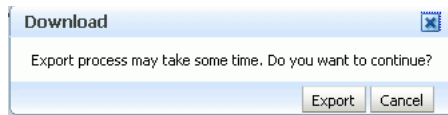
Table 39–1 Spaces Application Export Options

Field	Description
Include Services Data	<p>Select to export data stored in the WebCenter Portal repository for the following services: Activity Streams, Events, Feedback, Lists, Links, Message Boards, Connections, and Profiles. Notes 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 (and import) the WebCenter Portal schema data instead. For example:</p> <pre>DB_ORACLE_HOME/bin/expdp \"sys/password@serviceid as sysdba\" OWNER=srcrcuprefix_WEBCENTER DUMPFIL= /tmp/WCS.dmp STATISTICS=none</pre> <pre>DB_ORACLE_HOME/bin/impdp \"sys/password@serviceid as sysdba\" remap_schema=srcrcuprefix_WEBCENTER:tgtrcuprefix_WEBCENTER remap_tablespace=source_tablespace:target_tablespace DUMPFIL= /tmp/WCS.dmp STATISTICS=none TRANSFORM=oid:n</pre> <p>For details, refer to the <i>Oracle Database Utilities</i> guide.</p> <p>Deselect this option if you do not want to export any data associated with lists, events, tags, links, connections, profiles, message boards, activity streams, and feedback. 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>Note: 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), Personal Events, and Documents. To learn how to move data associated with these services, see documentation for that product. See also, Section 39.1.3, "Migrating Back-end Components for an Entire Spaces Application."</p>

Table 39–1 (Cont.) Spaces Application Export Options

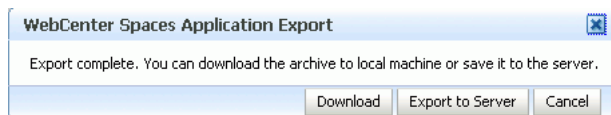
Field	Description
Include Customizations	<p>Select to export application customizations. For information about which application customizations are optional on export, see Table 39–4 and Table 39–5.</p> <p>If you deselect this option, WebCenter Portal: Spaces is exported without these application customizations.</p> <p>Portlet and page customizations are always exported. See also Figure 39–1, "Information Exported with a Spaces Application".</p>

- Click **Export**.
- In the Download dialog, as shown in [Figure 39–4](#), click **Export** to confirm that you want to go ahead.

Figure 39–4 Downloading an Export Archive

Progress information is displayed during the export process. The application being exported cannot be accessed during export operations.

- When the export process is complete, specify a location for the export archive (.ear).

Figure 39–5 Saving an Export Archive

Select one of:

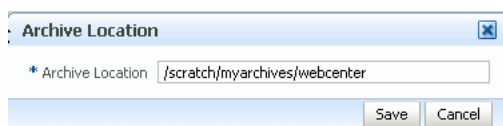
- Download** - Saves the export EAR file to your local file system.

Your Browser downloads and saves 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.

When the Archive Location dialog box displays ([Figure 39–6](#)), enter a suitable path for **Server Location**, for example, /tmp, and then click **Save**. The name of the EAR is not required here.

Ensure that the server directory you specify has write permissions.

Figure 39–6 Archive Location

- Click **Close** to dismiss the Export window.

The export archive (.EAR) is saved to the specified location.

Check the diagnostic log file, `WC_Spaces-diagnostic.log`, for any warnings or errors reported during the export process. To view the log file, choose the menu option **WebCenter > Logs > View Log Messages**. For details, see Section 34.3, "Viewing and Configuring Log Information". See also [Section 39.5, "Troubleshooting Import and Export Issues for Spaces."](#)

39.1.4.2 Exporting the Spaces Application Using WLST

Use the WLST command `exportWebCenterApplication` to export the Spaces application. For command syntax and examples, see "exportWebCenterApplication" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

The Spaces application is temporarily unavailable during export operations to prevent data conflicts. Any user who tries to login or access a Spaces page sees an "application unavailable" page.

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

39.1.5 Importing an Entire Spaces Application

This section describes how to import an entire Spaces application using Fusion Middleware Control and WLST commands.

Before importing the Spaces application:

- Migrate back-end components for the application, such as the LDAP identity store, credential store, policy store, discussions server, content server, Oracle WebLogic Communications Server, portlet producers, and so on. See [Section 39.1.3, "Migrating Back-end Components for an Entire Spaces Application."](#)

Personal pages, that is, pages users create in the Home space, are only migrated if the target and source applications both use the same LDAP identity store; this is because personal page assignments are per user GUID.

- Oracle also recommends that you backup the database schema, WebCenter Portal repository, MDS, and your policy store. See [Section 39.4, "Backing Up and Recovering WebCenter Portal Applications."](#)
- Check that all users assigned to the `Administrator` role exist in the target identity store. On import, users listed in the 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 29.5, "Moving the Administrator Account to an External LDAP Server."](#)
- Confirm that the Spaces archive (.ear) that you want to import was exported from WebCenter Spaces 11.1.1.4.0 or later. You cannot import archives from earlier versions (such as 11.1.1.2.0 or 11.1.1.3.0) directly into WebCenter Spaces 11.1.1.4.0. If necessary, you must upgrade to 11.1.1.4.0 before you create the export archive. For details, "Patching Oracle WebCenter" in *Oracle Fusion Middleware Patching Guide*.

The Spaces application is temporarily unavailable during import and export operations to prevent data conflicts. Any user who tries to login or access a Spaces page sees an "application unavailable" page.

This section includes the following:

- [Section 39.1.5.1, "Importing a Spaces Application Using Fusion Middleware Control"](#)
- [Section 39.1.5.2, "Importing a Spaces Application Using WLST"](#)
- [Section 39.1.5.3, "Verify an Imported Spaces Application"](#)

39.1.5.1 Importing a Spaces Application Using Fusion Middleware Control

Fusion Middleware administrators can import an entire WebCenter application using Fusion Middleware Control.

To import a Spaces application using Fusion Middleware Control:

1. In Fusion Middleware Control, navigate to the home page for Spaces.
See [Section 6.2, "Navigating to the Home Page for the Spaces Application."](#)
2. From the **WebCenter Portal** menu, select **Application Import**.
3. In the Spaces Application Import page ([Figure 39–7](#)), specify the location of your Spaces application archive (.ear). Select one of the following:
 - **Archive Located on Local File System** - Enter the **Archive 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 **Archive Location**. Any shared location accessible from this Spaces application.

The archive you select must contain an entire Spaces application export—you cannot import individual spaces from here. Refer to "Exporting and Importing Spaces and Space Templates" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces* for more information.

Figure 39–7 Spaces Application Import Page

4. Click **Import**.
5. In the Spaces Application Import dialog ([Figure 39–8](#)), click **Import**.

Figure 39–8 Spaces Application Import dialog

Once the import is complete, a success message displays.

After importing an entire Spaces application, log in and verify the application. For details, see [Section 39.1.5.3, "Verify an Imported Spaces Application"](#).

39.1.5.2 Importing a Spaces Application Using WLST

Use the WLST command `importWebCenterApplication` to import a Spaces application. For command syntax and examples, see "importWebCenterApplication" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

Note: After importing an entire Spaces application, log in and verify the application. For details, see [Section 39.1.5.3, "Verify an Imported Spaces Application"](#).

39.1.5.3 Verify an Imported Spaces Application

After importing an entire Spaces application you must:

1. Restart the managed server on which the newly imported Spaces application is deployed.

In a cluster environment, restart each managed server in the cluster. See also, [Section 8.2, "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments."](#)

2. Log in to the Spaces application and verify that all spaces and space templates are available as expected.

If not, see [Section 39.5.2, "Spaces and Space Templates Not Available After Import"](#).

3. Initiate the Oracle Secure Enterprise Search crawler to index newly imported data.

See also, *Oracle Secure Enterprise Search Administrator's Guide*.

39.1.6 Prerequisites for Individual Space Export and Import

To export one or more spaces, the Spaces application that contains the spaces must be up and running, and all the spaces you want to export must be offline to prevent data conflicts. For details, see, "Taking Any Space Offline" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*. If a space contains Web Service data controls or portlets, all associated Web Services or producers must also be up and accessible for the export and import to succeed.

Space-related data associated with some back-end components, specifically the discussions server, must be migrated *after* you export or import spaces. See next section, [Section 39.1.7, "Migrating Back-end Components for Individual Spaces."](#)

Note: The simultaneous export or import of large numbers of spaces is not recommended as, depending on server configuration, it may affect system performance. If a serious deterioration in performance is observed, break-down the export or import into several smaller groups.

39.1.7 Migrating Back-end Components for Individual Spaces

When migrating one or more spaces, you must also migrate the back-end components used by the space. This section tells you how.

This section includes the following sub sections:

- [Section 39.1.7.1, "Exporting Discussions for a Space"](#)
- [Section 39.1.7.2, "Importing Discussions for a Space"](#)
- [Section 39.1.7.3, "Exporting Documents for a Space"](#)
- [Section 39.1.7.4, "Importing Documents for a Space"](#)
- [Section 39.1.7.5, "Exporting/Importing Space Documents using the Document Migration Utility"](#)

You must import the spaces on to the target *before* importing these back-end components.

39.1.7.1 Exporting Discussions for a Space

Use the Discussions Server Admin Console to export discussions associated with a particular space.

Space discussions are exported to an .xml file, and saved to a .zip file in the DOMAIN_HOME/config/fmwconfig/servers/<target_server_name>/owc_discussions/data/ directory.

Where DOMAIN_HOME is the path to the Oracle WebLogic Server domain. For example, MW_HOME/user_projects/domains/my_domain/config/fmwconfig/servers/WC_Collaboration/owc_discussions/data/.

To export discussions for a space:

1. Login to the 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 Spaces as follows:

- a. Login to Spaces with administrative privileges, and open the Spaces administration pages.

See "Accessing Spaces Administration Pages" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

- b. Click **Spaces**.
- c. Select the space you want to export, then choose **Edit Space** from the **Edit** menu.
- d. Click **Services**, then **Discussions**.
- e. Note down the **Forum Name/ID** or **Category Name/ID** associated with this Space.

WebCenter Portal's 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 space, to point to the new ID. For details, see [Section 39.1.9.1, "Importing Individual Spaces Using the Spaces Application"](#) - Step 11.

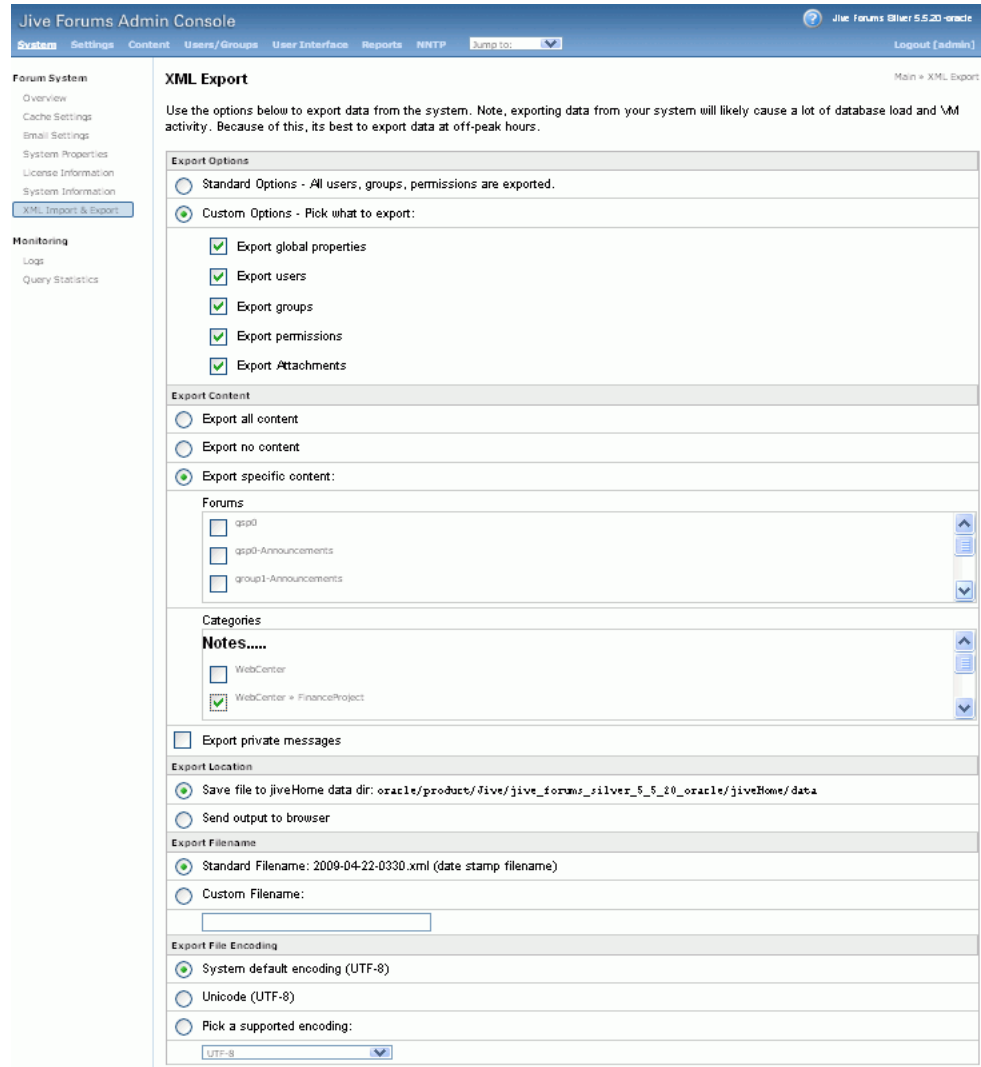
- f. Click **Forum Administration**, and login to the Admin Console.
2. In the Admin Console, select the **System** menu and choose **XML Export & Import** in the sidebar.
3. Select **Data Export**.
4. Set the following options ([Figure 39-9](#)):

- 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: Spaces that support multiple forums use a category to store discussions. Other spaces use a single forum.

- c. **Export location, Export filename, Export file encoding** - Keep the default values.

Figure 39–9 Exporting Discussions for an Individual Space



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/config/fmwconfig/servers/<server_name>/owc_discussions/data directory to same location on the target discussions server.

For example,
 MW_HOME/user_projects/domains/my_domain/config/fmwconfig/servers/WC_Collaboration/owc_discussions/data.

Before importing space discussions on the target system, the space you are migrating must exist on the target. See [Section 39.1.9.1, "Importing Individual Spaces Using the Spaces Application."](#)

39.1.7.2 Importing Discussions for a Space

Use the Discussions Server Admin Console to import discussions exported from another WebCenter Spaces application.

Ensure that the associated space exists on the target before you import the discussion data. See [Section 39.1.9.1, "Importing Individual Spaces Using the Spaces Application."](#)

Note: WebCenter Portal's 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 exist on both systems. When ID clashes occur, the imported forum (or category) is assigned a new, unique ID and therefore you must reconfigure the space to point to the new ID. See Step 11 below for details.

To import discussions for a particular space:

1. Log into the 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, log in through Spaces as follows:

- a. Log into Spaces with administrative privileges, and open the Spaces administration pages.
See "Accessing Spaces Administration Pages" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.
 - b. Click **Spaces**.
 - c. Select the space for which you want to import data, and then choose **Edit Space** from the **Edit** menu.
 - d. Click **Services**, then **Discussions**.
 - e. Click **Forum Administration** (on the far right), and log into 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 space export file from the list available ([Figure 39-10](#)).

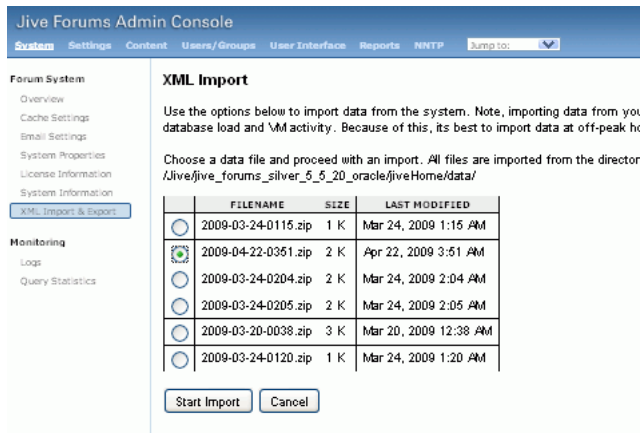
If the file you want is not listed, copy the export .zip file from the source directory

`DOMAIN_HOME/config/fmwconfig/servers/<target_server_name>/owc_discussions/data/` to same location on this target. See also, [Section 39.1.7.1, "Exporting Discussions for a Space."](#)

Where DOMAIN_HOME is the path to the Oracle WebLogic Server domain. For example,

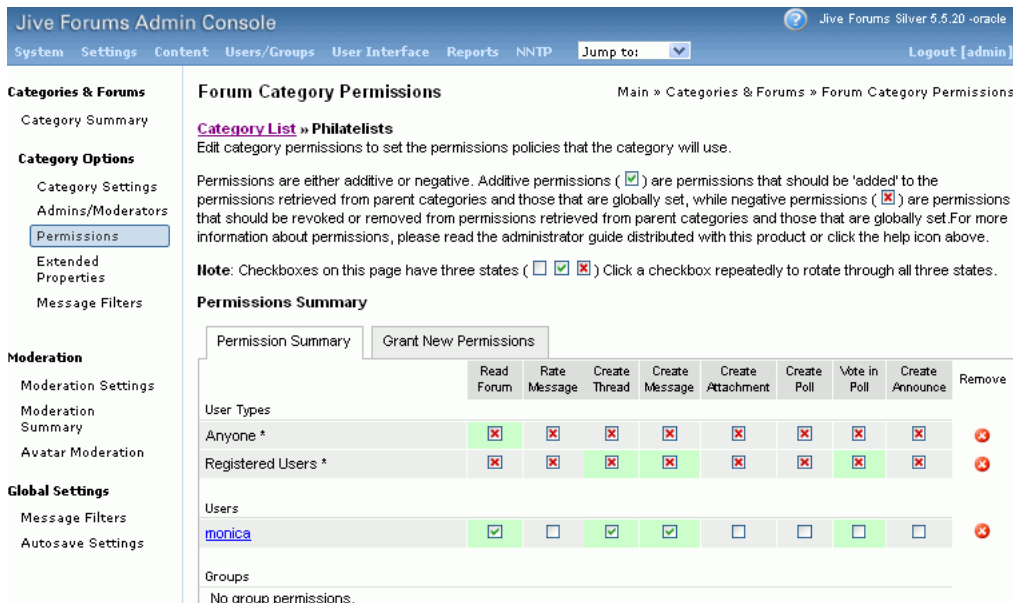
`MW_HOME/user_projects/domains/my_domain/config/fmwconfig/servers/WC_Collaboration/owc_discussions/data/`.

Figure 39–10 Importing Discussions for a Space



5. Click **Start Import**.
On import, the discussions data is copied to the discussions server. In the next step you reassociate the 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 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 39–11).

Figure 39–11 Editing Forum Permissions



11. In the Spaces application, navigate to the space's Discussions Forum Settings tab, to reassociate the space with the discussion data that you just imported:
 - a. Log into Spaces with administrative privileges.
See "Accessing Spaces Administration Pages" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.
 - b. Open Spaces Administration.
 - c. Click **Spaces**.
 - d. Select the space for which you want to import data, and then choose **Edit Space** from the **Edit** menu.
 - e. Click **Services**, 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**.

39.1.7.3 Exporting Documents for a Space

You are not required to export space-related documents *before* you export a space, because the documents remain in the source content repository. After migrating your space to another Spaces application you can use WebCenter Portal's Document Migration Utility to export documents from the source space and import them to the new target space. For detailed steps, see [Section 39.1.7.5, "Exporting/Importing Space Documents using the Document Migration Utility."](#)

39.1.7.4 Importing Documents for a Space

There are several ways to import documents into a space:

- In the Spaces application, open the space, and on the Documents page or in a Document Manager, Document Explorer, or Folder Viewer task flow, use the **Upload** action to import one or more files at a time, as described in "Uploading New Files" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.
- When the content repository is Oracle WebCenter Content Server:
 - **Use WebCenter Portal's Document Migration Utility**, as described in [Section 39.1.7.5, "Exporting/Importing Space Documents using the Document Migration Utility"](#).
Use this utility to migrate all files/folders stored for one or more spaces on Oracle WebCenter Content Server. When you migrate documents using this utility, most document metadata, including whether the file is a wiki or a blog, is preserved.
 - **Use the Batch Loader utility**, as described in "Batchloading Content" in *Oracle WebCenter Content System Administrator's Guide for Content Server*.
Use the Batch Loader to migrate space-related documents if you want to preserve document metadata or require document links in Content Presenter task flows to work postimport.
 - **Use WebDAV**, which is installed with Oracle WebCenter Content Server out-of-the-box, to drag and drop content from the folder belonging to the original space in your Content Server repository to the empty folder assigned

to the target space. When dragging and dropping content to the target system, **do not** drag the original space's *source folder* to the target; drag and drop only the content that is stored under the space's folder.

If you do not know the WebDAV URL for the Content Server that is used to store documents, contact your Fusion Middleware Administrator. If the base URL for that Content Server is `http://host:port/relative_web_root`, the WebDAV root URL is `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).

Specifically, **do not** use WebDAV if your space contains wikis/blogs. WebDav does not maintain custom metadata, so wikis/blogs are imported as HTML documents and appear broken in the target.

39.1.7.5 Exporting/Importing Space Documents using the Document Migration Utility

You can migrate all files and folders stored for a specific space (or a set of spaces) using WebCenter Portal's Document Migration Utility. You can use the same utility to migrate documents stored for space templates. There are three distinct phases to document migration:

- **First phase: Space migration to new target**
On import, the Documents service is enabled or disabled in the target to match that of the source. If the Documents service is enabled in the source, a folder is created on the target Oracle WebCenter Content Server for the space (or space template) and appropriate content server permissions are granted to users and groups with access to the space/space template.
- **Second phase: Document export**
When you export document content for a space (or space template), the current version of all the files/folders stored for the space on Oracle WebCenter Content Server are included in the export archive.
- **Third phase: Document import to new target**
On import the exact hierarchical structure of the files/folders is maintained. Metadata for the files/folders is also maintained wherever possible. Specifically, this means that wiki and blogs appear as wiki/blogs on the target.

This section describes the second/third phases. For information on the first phase (space/space template migration), see [Section 39.1, "Exporting and Importing a Spaces Application for Data Migration."](#) The Document Migration Utility exports space/space template documents into an archive which the utility can subsequently use to import the archived documents into the target.

The following information is not included in the export archive:

- **Home space content**
- **Version history** - Only the current revision is migrated
- **Renditions** - Renditions are recreated on import, as per settings on the target
- **Original create dates** - Create dates for all documents/folders reset to the date and time the documents are imported

- **Unknown doctypes** - Doctypes that do not exist on the target are set to the default doctype for the target
- **Comments on documents** - Comments that users enter about documents while working the Spaces application are stored with activity stream data, not as document metadata.
- **Links to documents** - Links that users create to documents are stored with link data, not as document metadata.

39.1.7.5.1 Properties Required to Run the Document Migration Utility Table 39–2 describes the properties required to run the Document Migration Utility. For information on how to run the utility, see [Section 39.1.7.5.2, "Migrating Content Using the Document Migration Utility."](#)

Table 39–2 Document Migration Properties

Property	Description	Requirement
Usage	Specifies whether you want to import or export content to a file. Options are: <code>import</code> and <code>export</code>	Export and Import
MDSConn	Specifies MDS JDBC connection in the format: <code>jdbc:oracle:thin:@host:port:SID</code> or <code>jdbc:oracle:thin:@host:port/ServiceName</code>	Export
MDSUser	Specifies the MDS user name used by the Spaces application	Export
MDSPwd	Specifies password for the MDS user. Only include to avoid password prompt.	Export
ExportScopes	Specifies the internal name of each space/space template with content to export. Separate multiple space/template names with a comma. Prefix space template names with <code>spacetemplate/<template_internal_name></code> . Ensure there are no spaces in the comma separated list. You can obtain internal names from the About Space and About Space Template dialogs. Do not enter display names here.	Export
UCMConn	Specifies Content Server URL in the format: <code>idc://host:intradocPort</code> When <code>usage=export</code> , specify the URL of the Content Server instance from which content is to be exported. When <code>usage=import</code> , specify the URL of the Content Server instance to which the content is to be imported.	Export and Import
UCMUser	Specifies the Content Server user name used to connect through RIDC.	Export and Import
UCMPwd	Specifies password for the Content Server user. Only include to avoid password prompt.	Export and Import
TmpDirPath	Optional. Temporary location for data extraction. If not specified, defaults to the system tmp directory.	Export and Import
ArchivePath	Document archive location.	Export and Import
ArchiveName	Optional. Name for the document archive (.zip). Default is <code>docsexport.zip</code> .	Export and Import

39.1.7.5.2 Migrating Content Using the Document Migration Utility To migrate documents for one or more spaces (or space templates), you can use any of the following methods:

- [Specifying Document Migration Properties in a Properties File](#)
- [Specifying Document Migration Properties on the Command Line](#)
- [Specifying Document Migration Properties on the Command Line When Prompted](#)

What You Should Do/Know Before Migrating Content:

1. Migrate the required spaces/space templates to the target application.

For details, see [Section 39.1.9, "Importing Individual Spaces"](#) or [Section 39.1.12, "Importing Space Templates"](#).

2. Navigate to: `WEBCENTER_ORACLE_HOME/webcenter/archives`

This directory contains the Document Migration Utility, `content-migration-tool.jar`.

When exporting documents, remember that a document archive (.zip) is created at the location you specify in the `archivePath` property.

When importing documents, the document content in the export archive (specified as the `archivePath` property) is uploaded to the target Content Server. To verify this, log in to the Spaces application, navigate to the space (or space template) and verify that the imported content is available as expected.

Specifying Document Migration Properties in a Properties File

1. Create a properties file containing all the properties required for your export/import. See [Table 39-2](#) for a description of all the properties.
 - a. Copy and paste the following properties file into Notepad or another suitable text editor, then edit according to your environment:

```
# Document migration properties for one or more spaces.

# Specify whether you want to export content to a file or
# import content from an archive to another content repository
# valid values: export | import
Usage=export

# Specify connection details for Oracle WebCenter Content repository:
#   UCMConn - Content Server URL. Format: idc://host:intradocPort
#   UCMUser - Content Server user name used to connect through RIDC
#   UCMPwd - Password for UCMUser. Only include to avoid password prompt
# Required for: Export and Import

UCMConn=idc://mycontentserver.mycompany.com:9444
UCMUser=weblogic
#UCMPwd=welcome1

# Specify a temp directory and name/location for the export archive
#   TmpDirPath -Optional. Temporary location for data extraction.
#               If not specified, defaults to the system temporary
#               directory.
#   ArchiveName -Optional. Name for the document archive (.zip).
#               Default is docsexport.zip.
#   ArchivePath -Document archive location
# Required for: Export and Import
```

```

TmpDirPath=/scratch/user1/migrateMySpaceDocs/tmpdir
ArchivePath=/scratch/user1/migrateMySpaceDocs/output
ArchiveName=myspacedocs.zip

# Specify MDS details (export only)
# MDSConn - MDS JDBC connection. Format:
#           jdbc:oracle:thin:@host:port:SID or
#           jdbc:oracle:thin:@host:port/ServiceName
# MDSUser - MDS schema user name used by the Spaces application
# MDSPwd = Password for MDSUser. Only include to avoid password prompt
# Required for: Export

MDSConn=jdbc:oracle:thin:@mymdshost.mycompany.com:1521:wkcdb01
MDSUser=user1_mds
#MDSPwd=welcome1

# Specify the internal name of each space/space template with content to
export.
# Separate multiple space/template names with a comma.
# Use internal names only. Do not enter display names.
# Obtain internal names from "About Space" and "About Space Template"
dialogs.
# Prefix space template names with 'spacetemplate/<template_internal_name>'
# as indicated in the example.
# Required for: Export

ExportScopes=MySpace1,MySpace2,spacetemplate/MySpaceTemplate

```

- b. Save the file. For example, save as `myMigrationProperties.properties` or similar.
2. Navigate to the `WEBCENTER_ORACLE_HOME/webcenter/archives` directory in which the Document Migration Utility, `content-migration-tool.jar` is located.
3. Run the Document Migration Utility by specifying the absolute path to your document migration properties file on the command line (Example 39–11):

```

java -jar content-migration-tool.jar
<absolute_path_to_migrationPropertiesFilename>

```

Optionally, specify logging settings using the `java.util.logging.config.file` parameter as described in [Section 39.1.7.5.3, "Running the Document Migration Utility with Additional Logging."](#)

Example 39–11 Specifying Document Migration Properties in a Properties File

```

java -jar content-migration-tool.jar /home/user1/myMigrationProperties.properties

```

Running the Document Migration Utility with the following settings:

```

Usage           = export
UCM Connection  = idc://mycontentserver.mycompany.com:9444
UCM User       = weblogic
Archive fullname = /scratch/user1/migrateMySpaceDocs/output/myspacedocs.zip
Scopes to Export = [mySalesSpace, spacetemplate/SalesTemplate]
MDS Connection  = jdbc:oracle:thin:@mymdshost.mycompany.com:1521:wkcdb01
MDS User       = user1_mds
Setting up MDS connection
Connection to MDS created successfully

```


Specifying Document Migration Properties on the Command Line

1. Navigate to the `WEBCENTER_ORACLE_HOME/webcenter/archives` directory in which the Document Migration Utility, `content-migration-tool.jar` is located.
2. Run the Document Migration Utility by specifying individual properties on the command line:

To export content:

```
java -jar content-migration.jar Usage UCMConn UCMUser TmpDirPath ArchivePath
ArchiveName MDSConn MDSUser ExportScopes [UCMPwd MDSPwd]
```

To import content:

```
java -jar content-migration.jar Usage UCMConn UCMUser TmpDirPath ArchvePath
ArchiveName [UCMPwd]
```

Note: You can, optionally, specify the `UCMPwd` and `MDSPwd` parameters on the command line. If you do not do so, you are prompted to provide them.

Optionally, specify logging settings using the `java.util.logging.config.file` parameter, as described in [Section 39.1.7.5.3, "Running the Document Migration Utility with Additional Logging."](#)

Example 39–12 exports a space called `MySalesSpace` and a space template called `SalesTemplate`.

Example 39–12 Specifying Document Migration Properties on the Command Line For an Export

```
java -jar content-migration-tool.jar export
idc://mycontentserver.mycompany.com:9444
weblogic /scratch/user1/migrateMySpaceDocs/tmpdir
/scratch/user1/migrateMySpaceDocs/output/myspacedocs.zip
jdbc:oracle:thin:@mymdshost.mycompany.com:1521:wkcdb01 user1_mds
[mySalesSpace, spacetemplate/SalesTemplate] mypassword mypassword
```

Running the Document Migration Utility with the following settings:

```
Usage           = export
UCM Connection  = idc://mycontentserver.mycompany.com:9444
UCM User       = weblogic
Archive fullname = /scratch/user1/migrateMySpaceDocs/output/myspacedocs.zip
Scopes to Export = [mySalesSpace, spacetemplate/SalesTemplate]
MDS Connection  = jdbc:oracle:thin:@mymdshost.mycompany.com:1521:wkcdb01
MDS User       = user1_mds
```

Setting up MDS connection

```
INFO: Export completed successfully. Export archive located at
/scratch/user1/migrateMySpaceDocs/output/myspacedocs.zip
```

Specifying Document Migration Properties on the Command Line When Prompted

1. Navigate to the `WEBCENTER_ORACLE_HOME/webcenter/archives` directory in which the Document Migration Utility, `content-migration-tool.jar` is located.
2. Run the Document Migration Utility by specifying the properties on the command line when prompted:


```
java -jar content-migration.jar
```

Optionally, specify logging settings using the `java.util.logging.config.file` parameter, as described in [Section 39.1.7.5.3, "Running the Document Migration Utility with Additional Logging."](#)

[Example 39–13](#) exports a space called `MySalesSpace` and a space template called `SalesTemplate`.

Example 39–13 Specifying Document Migration Properties on the Command Line When Prompted

```
java -jar content-migration-tool.jar

Enter the usage ('export' or 'import'): export
Enter UCM Connection (idc://<host name>:<socket port>):
idc://mycontentserver.mycompany.com:9444
Enter UCM User: weblogic
Enter UCM Password: mypassword
Enter the full path to the temporary directory:
/scratch/user1/migrateMySpaceDocs/tmpdir
Enter path to the directory where the export archive is to be created:
/scratch/user1/migrateMySpaceDocs/output/
Enter the name of the export archive to create (default = docsexport.zip):
myspacedocs.zip
Enter MDS Spaces Data Source Connection (jdbc:oracle:thin:@<host name>:<jdbc
port>:<SID>): jdbc:oracle:thin:@mymdshost.mycompany.com:1521:wkcdb01
Enter MDS Spaces Data Source User: user1_mds
Enter MDS Spaces Data Source Password: welcome1
Enter a comma separated list of scopes to export:
[mySalesSpace, spacetemplate/SalesTemplate]
Running Document Migration Utility with the following settings:
Usage = export
UCM Connection = idc://mycontentserver.mycompany.com:9444
UCM User = weblogic
Archive fullname = /scratch/user1/migrateMySpaceDocs/output/myspacedocs.zip
Scopes to Export = [mySalesSpace, spacetemplate/SalesTemplate]
MDS Connection = jdbc:oracle:thin:@mymdshost.mycompany.com:1521:wkcdb01
MDS User = user1_mds
Setting up MDS connection
INFO: Export completed successfully. Export archive located at
/scratch/user1/migrateMySpaceDocs/output/myspacedocs.zip
```

39.1.7.5.3 Running the Document Migration Utility with Additional Logging You can optionally run the Document Migration Utility with additional logging using the `java.util.logging.config.file` parameter as follows:

```
java -Djava.util.logging.config.file=<absolute_path_to_logging_properties_file>
-jar content-migration-tool.jar <migrationProperties>
```

Note: The `java.util.logging.config.file` parameter must be specified immediately after the `java` command and before `-jar`.

Where the `logging_properties_file` includes settings such as:

```
handlers=java.util.logging.ConsoleHandler.level=INFO
java.util.logging.ConsoleHandler.level=FINER
java.util.logging.ConsoleHandler.formatter=java.util.logging.SimpleFormatter
oracle.webcenter.doclib.level=INFO
```

39.1.8 Exporting Individual Spaces

Administrators can export one or more spaces from Spaces Administration pages or using WLST commands.

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 space archives to your local file system or to a remote server file system.

For more information about what is exported, see [Section 39.1.1, "Understanding Spaces Export and Import."](#)

The export process does not include data associated with external services, such as, Discussions, Announcements, and Documents. To learn how to move data associated with these services, see [Section 39.1.7, "Migrating Back-end Components for Individual Spaces."](#)

Individual spaces are locked during an export operation to prevent simultaneous imports/exports of the same space. If someone else is exporting a particular space, all subsequent attempts to export (or import) the same space are blocked. If a space contains Web Service data controls, all the associated Web Services must be up and accessible for the export to succeed.

Note: Space artifacts must be located in the shared *content directory* to be exported. For example, icons and images associated with a page template must be placed in the page template's content directory to be exported. For more information, see "What You Should Know About a Resource's Properties" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

Out-of-the-box templates and user customizations are never exported. For information on user customizations, see the section "What You Should Know About Customizing Page Components" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

This section includes the following:

- [Section 39.1.8.1, "Exporting Individual Spaces Using the Spaces Application"](#)
- [Section 39.1.8.2, "Exporting Individual Spaces Using WLST"](#)

If you want to export an entire Spaces application, see [Section 39.1.4, "Exporting an Entire Spaces Application."](#)

39.1.8.1 Exporting Individual Spaces Using the Spaces Application

Administrators can export one or more spaces from Spaces Administration pages. For details, see "Exporting Spaces" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

39.1.8.2 Exporting Individual Spaces Using WLST

Use the WLST command `exportGroupSpaces` to export one or more 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 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

39.1.9 Importing Individual Spaces

Administrators can import a space archive (.EAR) from the Spaces application or using WLST commands.

On import, *all* spaces included in the archive are created or re-created on the target application. Existing spaces are deleted then replaced, and new spaces are created.

If you intend to import spaces with names identical to those available on the target application, ensure that those spaces are offline in the target application. It is not possible to overwrite a space, on import, if it is online. For details, see "Taking Any Space Offline" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

Spaces are locked during an import operation to prevent simultaneous imports/exports of the same space. If someone else is importing a particular space, all subsequent attempts to import (or export) the same space are blocked. If a space contains Web Service data controls, all the associated Web Services must be up and accessible for the import to succeed.

All spaces must have a security policy. Therefore, when you import a brand new space you must ensure that import the space's security policy too. Existing spaces 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.

When you import a space with security, security policy updates do not apply immediately. Any user logged in to the Spaces application must log out and log back in to adopt the new space security policy.

If data migration is important, documents and discussions can be migrated for individual spaces. For details, see [Section 39.1.7, "Migrating Back-end Components for Individual Spaces."](#)

This section includes the following:

- [Section 39.1.9.1, "Importing Individual Spaces Using the Spaces Application"](#)
- [Section 39.1.9.2, "Importing Individual Spaces Using WLST"](#)

After importing one or more spaces, consider initiating an Oracle Secure Enterprise Search crawl to index the newly imported data.

39.1.9.1 Importing Individual Spaces Using the Spaces Application

Administrators can import archives containing one or more spaces (.EAR) into another Spaces application. For details, see, "Importing Spaces" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

39.1.9.2 Importing Individual Spaces Using WLST

Use the WLST command `importGroupSpaces` to import one or more 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 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

39.1.10 Migrating Back-end Components for Space Templates

Space templates can contain pages, portal resources, documents, discussions, lists, and member details. Most template data is exported along with the template, there is no need to migrate template data separately when exporting and importing space templates.

You must, however, migrate the space template's folder and content (on Oracle WebCenter Content Server) to the target instance as described below. If you do not, the Documents service is not enabled in any space that you create, using this template.

Importing the Back-end Folder and Documents for a Space Template

Use WebCenter Portal's Document Migration Utility to migrate document content for space templates. For details, see [Section 39.1.7.5, "Exporting/Importing Space Documents using the Document Migration Utility"](#).

39.1.11 Exporting Space Templates

Administrators can export space templates and import them into other Spaces applications. Out-of-the-box templates cannot be exported.

Space templates can include pages, resources, documents, discussions, lists, service information, and security information such as custom roles and current members.

While export and import utilities are primarily used to move information between Spaces applications, the space template export feature is also useful as a backup service, and for sharing and exchanging templates with others.

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 space security policy information.

You can save export archives to your local file system or to a remote server file system.

This section includes the following:

- [Section 39.1.11.1, "Exporting Space Templates Using the Spaces Application"](#)
- [Section 39.1.11.2, "Exporting Space Templates Using WLST"](#)

See also, [Section 39.1.10, "Migrating Back-end Components for Space Templates."](#) and [Section 39.1.8, "Exporting Individual Spaces."](#)

39.1.11.1 Exporting Space Templates Using the Spaces Application

Spaces administrators can export one or more space templates from Spaces Administration pages. For details, see "Exporting Space Templates" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

39.1.11.2 Exporting Space Templates Using WLST

Use the WLST command `exportGroupSpaceTemplates` to export one or more 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 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

39.1.12 Importing Space Templates

Administrators can import a space template archive (.EAR) into another Spaces application.

On import, *all* space templates included in the archive are re-created on the target application. If a space template exists on the target, then it is deleted and replaced. If a space template does not exist, then it is created.

Newly imported space templates are not immediately available for general use. You must publish the imported templates to make them available to everyone. See "Publishing and Hiding Space Templates" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

This section includes the following:

- [Section 39.1.12.1, "Importing Space Templates Using the Spaces Application"](#)
- [Section 39.1.12.2, "Importing Space Templates Using WLST"](#)

See also, [Section 39.1.9, "Importing Individual Spaces"](#)

39.1.12.1 Importing Space Templates Using the Spaces Application

Spaces administrators can import one or more space templates from Spaces administration pages. For details, see "Importing Space Templates" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

39.1.12.2 Importing Space Templates Using WLST

Use the WLST command `importGroupSpaces` to import one or more 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 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

39.1.13 Exporting Spaces Resources

Authorized users can download Spaces resources, such as skins and page templates, while the application is running, edit and extend them in tools such as Oracle JDeveloper, and then upload them back into their Spaces application. Users who want to share or migrate resources to other Spaces applications can use the download feature too.

You can download the following application-level and space-level resources through the resource management pages in Spaces:

- Skins
- Page Styles
- Page Templates
- Content Display Templates
- Navigations
- Resource Catalogs
- Task Flows
- Mashup Styles

Alternatively, administrators can perform the same task using WLST commands.

When you download (or export) a WebCenter Portal resource, the resource details are saved to a WebCenter Portal export archive (.EAR). You can save the export archive to your local file system or a remote server file system using a filename of your choice.

This section includes the following:

- [Section 39.1.13.1, "Exporting WebCenter Resources Using the Spaces Application"](#)
- [Section 39.1.13.2, "Exporting WebCenter Resources Using WLST"](#)

39.1.13.1 Exporting WebCenter Resources Using the Spaces Application

Spaces administrators and individual space moderators can export resources from WebCenter Portal resource administration pages. For details, see "Downloading a Resource" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

39.1.13.2 Exporting WebCenter Resources Using WLST

Use the WLST command `exportWebCenterResource` to export a single WebCenter Portal resource. For command syntax and examples, see "exportWebCenterResource" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

39.1.14 Importing Space Resources

Authorized users can import (upload when using WLST) portal resources, such as skins and page templates, while the application is running. You can import the following application-level and space-level resources through the resource management pages or using WLST commands:

- Skins
- Page styles
- Page templates
- Content display templates
- Navigations
- Resource catalogs
- Task flows
- Mashup styles

You can only import a resource previously saved to a WebCenter Portal export archive file (.EAR). For details, see [Section 39.1.13, "Exporting Spaces Resources"](#).

On import:

- *Existing portal resources* are overwritten, that is, resources with the same internal ID.
- *Space-level portal resources* are always imported back into the same space. You cannot import a resource into a different space.

This section includes the following:

- [Section 39.1.14.1, "Importing WebCenter Resources Using the Spaces Application"](#)
- [Section 39.1.14.2, "Importing WebCenter Resources Using WLST"](#)

39.1.14.1 Importing WebCenter Resources Using the Spaces Application

Spaces administrators and individual space moderators can import resources from WebCenter Portal resource administration pages. For details, see "Uploading a Resource" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

39.1.14.2 Importing WebCenter Resources Using WLST

Use the WLST command `importWebCenterResource` to import a single WebCenter Portal resource. For command syntax and examples, see "importWebCenterResource" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

39.2 Exporting and Importing Framework Applications for Data Migration

This section describes how to export and import metadata and application customizations for portal applications developed using Oracle WebCenter Portal: Framework - referred throughout as *Framework applications*.

It includes the following sections:

- [Section 39.2.1, "Understanding Framework Application Export and Import"](#)
- [Section 39.2.2, "Prerequisites for Framework Application Export and Import"](#)
- [Section 39.2.3, "Exporting Portlet Client Metadata \(Framework Applications\)"](#)
- [Section 39.2.4, "Importing Portlet Client Metadata \(Framework Applications\)"](#)
- [Section 39.2.5, "Exporting WebCenter Portal Resources \(Framework Applications\)"](#)
- [Section 39.2.6, "Importing WebCenter Portal Resources \(Framework Applications\)"](#)
- [Section 39.2.7, "Exporting WebCenter Portal Service Metadata and Data \(Framework Applications\)"](#)
- [Section 39.2.8, "Importing WebCenter Portal Service Metadata and Data \(Framework Applications\)"](#)
- [Section 39.2.9, "Migrating Security for WebCenter Portal Applications"](#)
- [Section 39.2.10, "Migrating Data \(WebCenter Portal Applications\)"](#)

39.2.1 Understanding Framework Application Export and Import

Several migration tools are available to export and import Framework application, their connections and customizations (that is, customizations applied to an application, pages, and portlets) between stage and production environments ([Figure 39–12](#)).

Figure 39–12 WebCenter Portal Application Export and Import

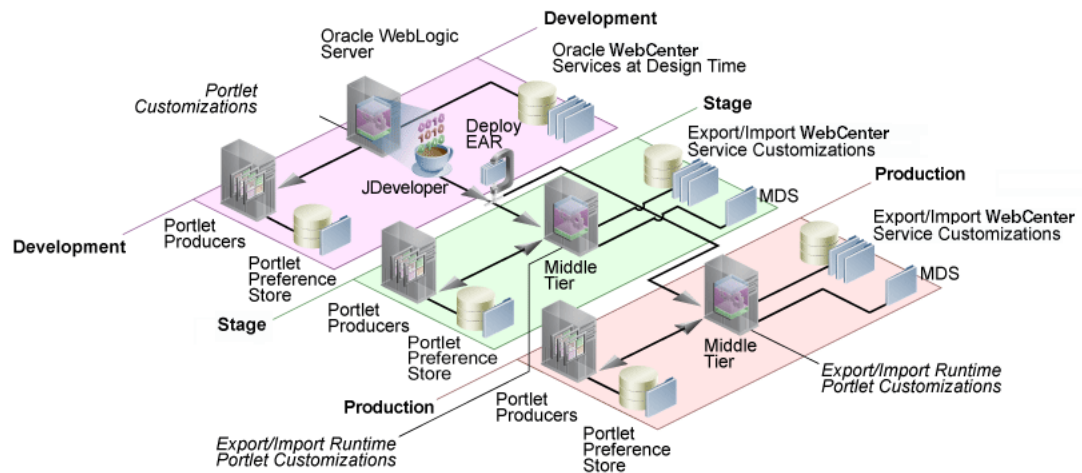


Table 39–3 lists available migration tools and their capabilities. All customizations listed in Table 39–3 are migrated with Framework applications.

Table 39–3 WebCenter Portal: Framework Application Migration Tools

Migration Tools	Capabilities
Portlet Client WLST Commands	Enable export and import of portlet client metadata, and producer customizations and personalizations.
WebCenter Portal Resource WLST Commands	Enable export and import of WebCenter Portal resources, such as skins, page templates, and so on.
MDS WLST Commands	Enables export and import of: <ul style="list-style-type: none"> Framework application metadata including customizations made to pages and WebCenter Portal services Data stored in the <code>connections.xml</code> and <code>adf-config.xml</code> documents
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 Framework application data. For information, see the part "Oracle Data Pump" in the <i>Oracle Database Utilities</i> guide.
Non-Oracle database utilities	Refer to the database manufacturer's documentation for information about their data migration tools.

39.2.2 Prerequisites for Framework Application Export and Import

Before exporting or importing metadata and customizations for a Framework application, ensure the following:

- The database in which the application metadata and schema is stored is up and running.
- The target instance is configured with the same set of services as the source instance. Additional services can be configured in the target, if required, but minimally, service configuration in the source and target must match.
- The `jps.policystore.removal` parameter is set to `OFF` in your application's `weblogic-application.xml` so that policies are migrated on import:


```
<application-param>
  <param-name>jps.policystore.removal</param-name>
  <param-value>OFF</param-value>
</application-param>
```

If this option is not set, no policy information is imported. In some instances you may not want to migrate policy data, for example, when migrating from a test environment to a production environment where test data is not required. Note however, that pages created on the source instance at runtime do not display on the target instance because no page grants exist on the target.

39.2.3 Exporting Portlet Client Metadata (Framework Applications)

To export portlet client metadata and producer customizations and personalizations, for a Framework application, use the WLST command `exportPortletClientMetadata`. 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.

Note: Both the portlet producer and individual portlets must include an `<allow-export>` tag that is set to `true`. If this tag is not set, the portlet producer (and the portlets) are excluded from the export process. For details, refer to "How to Implement Export/Import of Customizations (WSRP 2.0)" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

For detailed syntax and examples, see "exportPortletClientMetadata" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.13.3.1, "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 Portal*.

39.2.4 Importing Portlet Client Metadata (Framework Applications)

This section describes how to import portlet client metadata and producer customizations and personalizations, for a Framework application, using the WLST command `importPortletClientMetadata`.

Prerequisites:

- The database in which the application metadata or schema is stored and the portlet producers must be up and running.
- Both the portlet producer and individual portlets must include an `<allow-import>` tag that is set to `true`. If the tag is not set, the portlet producer (and the portlets) are excluded from the import process. For details, refer to "How to Implement Export/Import of Customizations (WSRP 2.0)" in the *Oracle Fusion Middleware Developer's Guide for Oracle WebCenter Portal*.

To import portlet client metadata, run the WLST command `importPortletClientMetadata`:

```
importPortletClientMetadata(appName, fileName, [server, applicationVersion])
```

where:

- `appName`: Name of the Framework application (for example, `myWebCenterApp`).
- `fileName`: Name of the exported EAR file containing the portlet client metadata (for example, `myportletmetadata.ear`).
- `server`: Name of the managed server where the Framework application is deployed (for example, `WC_CustomPortal`).
- `applicationVersion`: Version number of the deployed application, if multiple versions of the application is deployed.

See also, [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

For detailed syntax and examples, see "importPortletClientMetadata" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*. See also, "Metadata Services (MDS) Custom WLST Commands".

39.2.5 Exporting WebCenter Portal Resources (Framework Applications)

Authorized users can download application resources, such as skins and page templates, while a Framework application is running, edit and extend them in tools such as Oracle JDeveloper, and then upload them back to the Framework application. Users who want to share or migrate resources to other Framework applications can use the download feature too.

You can download the following portal resources at runtime through the WebCenter Portal Administration Console:

- Skins
- Page Styles
- Page Templates
- Content Display Templates
- Navigations
- Resource Catalogs
- Task Flows
- Mashup Styles

When you download (or export) a WebCenter Portal resource, the resource details are saved to a WebCenter Portal export archive (.EAR). You can save the export archive to your local file system or a remote server file system using a filename of your choice.

For details, see [Section 36.5.8, "Downloading and Uploading a Resource"](#).

Alternatively, system administrators can perform the same task using the WLST command `exportWebCenterResource`. For command syntax and examples, see "exportWebCenterResource" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

39.2.6 Importing WebCenter Portal Resources (Framework Applications)

Authorized users can import application resources, such as skins and page templates, while a Framework application is running. You can import the following resources at runtime through the WebCenter Portal Administration Console:

- Skins

- Page Styles
- Page Templates
- Content Display Templates
- Navigations
- Resource Catalogs
- Task Flows
- Mashup Styles

You can import resources previously saved to WebCenter Portal export archive files (.ear), on your local or remote server file system. Existing resources, that is, resources with the same internal ID are overwritten on import.

For details, see [Section 36.5.8, "Downloading and Uploading a Resource"](#).

Alternatively, administrators can perform the same task using the WLST command `importWebCenterResource`. For command syntax and examples, see "importWebCenterResource" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

39.2.7 Exporting WebCenter Portal Service Metadata and Data (Framework Applications)

The metadata created by WebCenter Portal services is stored in the Oracle metadata store (MDS). For detailed information about MDS, see the chapter "Managing the Oracle Metadata Repository" in *Oracle Fusion Middleware Administrator's Guide*.

To export base documents for WebCenter Portal services, together with their customizations, use the WLST command `exportMetadata`.

For example:

```
exportMetadata(application='myWebCenterApp', server='WC_CustomPortal',
toLocation='/tmp/myrepos', docs='/oracle/webcenter/**')
```

Where:

- `application`: Name of the Framework application for which the metadata is to be exported (for example, `myWebCenterApp`).
- `server`: Server on which the Framework application is deployed (for example, `WC_CustomPortal`).
- `toLocation`: Target directory to which documents selected from the source partition are to be exported. The `toLocation` parameter can be used as a temporary file system for migrating metadata from one server to another.
- `docs`: List of comma separated fully qualified document name(s) and/or document name patterns (* and ** patterns).

In this example, "`docs='/oracle/webcenter/**'`" exports the required documents for *all* WebCenter Portal services storing metadata in MDS.

Note: The "docs= '/oracle/webcenter/**'" command *does not* export portlet customizations and personalizations or changes to configuration files such as `connections.xml` and `adf-config.xml`.

- To export portlet metadata, run the WLST command `exportPortletClientMetadata`. See also, [Section 39.2.3, "Exporting Portlet Client Metadata \(Framework Applications\)"](#).
 - To export configuration file updates that are stored in MDS, run the WLST command `exportMetadata` with "docs= '/META-INF/mdssys/cust/adfshare/adfshare/**' ". See also, [Appendix A.1.1, "adf-config.xml and connections.xml"](#).
-
-

For detailed syntax and examples, see "exportMetadata" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

Customizations listed in [Table 39–4](#) are also exported when Framework applications are migrated between stage and production environments.

Metadata for WebCenter Portal services, which consists of base and customization documents, are stored in the following paths:

- **Analytics:** `/oracle/webcenter/analytics/**`
- **Announcements:** `/oracle/webcenter/collab/announcement/**`
- **Blogs:** `/oracle/webcenter/blog/**`
- **Documents:** `/oracle/webcenter/doclib/**` and `/oracle/webcenter/doclib/view/jsf/fragments/**`
- **Discussions:** `/oracle/webcenter/collab/forum/**`
- **General Settings:** `/oracle/webcenter/generalsettings/**`
- **Events:** `/oracle/webcenter/collab/events/**`
- **External Applications:** `/oracle/webcenter/admin/**` and `oracle/adfinternal/extapp/**`
- **Instant Messaging and Presence:** `/oracle/webcenter/collab/rtc/**`
- **Links:** `/oracle/webcenter/relationship/**`
- **Language:** `/oracle/webcenter/webcenterapp/**`
- **Lists:** `/oracle/webcenter/list/**` and `/oracle/webcenter/list/view/jsf/regions/**`
- **Mail:** `/oracle/webcenter/collab/mail/**`
- **Navigations:** `/oracle/webcenter/navigationtaskflows/**`
- **Notes:** `/oracle/webcenter/note/**`
- **Page:** `/oracle/webcenter/page/**` and `/pageDefs/**`
- **Polls:** `/oracle/webcenter/collab/survey/**`
- **People Connections (Connections):** `/oracle/webcenter/peopleconnections/connection/**`

- **People Connections (Feedback):** /oracle/webcenter/peopleconnections/kudos/**
- **People Connections (Profile Gallery):** /oracle/webcenter/peopleconnections/personalweb/**
- **People Connections (Profile):** /oracle/webcenter/peopleconnections/profile/**
- **People Connections (Message Board):** /oracle/webcenter/peopleconnections/wall/**
- **Polls:** /oracle/webcenter/collab/survey/**
- **Recent Activity:** /oracle/webcenter/recentactivity/**
- **Resource Action Handler:** /oracle/webcenter/framework/service/**
- **RSS News Feed:** oracle/webcenter/rssviewer/**
- **Scope:** /oracle/webcenter/framework/scope/**
- **Search:** /oracle/webcenter/search/**
- **Security:** /oracle/webcenter/security/**
- **Smart Tag:** /oracle/webcenter/collab/smarttag/**
- **Space Browser:** /oracle/webcenter/community/**
- **Space Contacts:** /oracle/webcenter/people/**
- **Subscriptions:** /oracle/webcenter/notification/**
- **Tags:** /oracle/webcenter/tagging/**
- **adf-config.xml, connections.xml:**
/META-INF/mdssys/cust/adfshare/adfshare/**

Configuration file updates are not stored under the /oracle/webcenter/ directory alongside WebCenter Portal services. To export customizations associated with these files, run `exportMetadata` again with `"docs='META-INF/mdssys/cust/adfshare/adfshare/**'"`. See also, [Appendix A.1.1, "adf-config.xml and connections.xml"](#).

39.2.8 Importing WebCenter Portal Service Metadata and Data (Framework Applications)

To import WebCenter Portal service metadata and customizations for a Framework application, use the WLST command `importMetadata`. For example:

```
importMetadata(application='myWebCenterApp', server='WC_CustomPortal',
fromLocation='/tmp/myrepos', docs='/**')
```

Where:

- `application`: Name of the Framework application for which the metadata is be imported (for example, `myWebCenterApp`).
- `server`: Name of the target server on which the application is deployed (for example, `WC_CustomPortal`).
- `fromLocation`: Source directory from which documents are imported. The `fromLocation` parameter can be any temporary file system location for migrating metadata from one server to another.

- `docs`: List of comma separated fully qualified document name(s) and/or document name patterns (* and ** patterns).

For detailed syntax and examples, see "importMetadata" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

See also, [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

39.2.9 Migrating Security for WebCenter Portal Applications

Security migration involves moving the identity store, credential store, and policy store, from one WebCenter Portal application to another. The process is the same for all WebCenter Portal applications so you can follow the same instructions provided for the Spaces application:

- [Section 39.1.3.1, "Exporting the LDAP Identity Store"](#)
- [Section 39.1.3.2, "Importing the LDAP Identity Store"](#)
- [Section 39.1.3.3, "Exporting and Importing the LDAP Credential Store"](#)
- [Section 39.1.3.4, "Exporting and Importing the LDAP Policy Store"](#)

39.2.10 Migrating Data (WebCenter Portal Applications)

To export the WebCenter Portal application data, use the export and import database utilities. This section includes the following sub sections:

- [Section 39.2.10.1, "Exporting Data \(WebCenter Portal Applications\)"](#)
- [Section 39.2.10.2, "Importing Data \(WebCenter Portal Applications\)"](#)

39.2.10.1 Exporting Data (WebCenter Portal Applications)

To export WebCenter Portal application data, use the appropriate database utility:

- For an Oracle database, go to `ORACLE_HOME/bin` of your database and run the command described in [Example 39–14](#).
- For non-Oracle databases, refer to the manufacturer's documentation.

Example 39–14 Data Pump Utility (Export)

```
DB_ORACLE_HOME/bin/expdp \ "sys/password@serviceid as sysdba\"  
OWNER=srcrcuprefix_WEBCENTER FILE=/tmp/wc.dmp STATISTICS=none
```

where:

- `DB_ORACLE_HOME` is the directory in which the database for the Oracle WebCenter Portal schema is installed.
- `password` is the password for system database user.
- `serviceid` is the service ID of the database connection.
- `OWNER` is the schema to be exported. This is the RCU suffix that was used during installation along with the suffix `_WEBCENTER`. For example, `DEV_WEBCENTER`.
- `FILE` contains the exported data.

For more information, see "Oracle Data Pump" in the *Oracle Database Utilities* guide.

39.2.10.2 Importing Data (WebCenter Portal Applications)

To import WebCenter Portal application data, use the appropriate database utility:

- For an Oracle database, go to `ORACLE_HOME/bin` of your database and run the command described in [Example 39–15](#)
- For non-Oracle databases, refer to the manufacturer's documentation.

Example 39–15 Data Pump Utility (Import)

```
DB_ORACLE_HOME/bin/impdp \ "sys/password@serviceid as sysdba\"
remap_schema=srcrcuprefix_WEBCENTER:tgtrcuprefix_WEBCENTER
remap_tablespace=source_tablespace:target_tablespace DUMPFILE=/tmp/wc.dmp
STATISTICS=none TRANSFORM=oid:n
```

where:

- `DB_ORACLE_HOME` is the directory in which the database for the Oracle WebCenter Portal schema is installed.
- `password` is the password for system database user.
- `serviceid` is the service ID of the database connection.
- `REMAP_SCHEMA` identifies the source and target schemas. For example, schema names include the RCU suffix that was used during installation, `_WEBCENTER`, along with the user supplied prefix. For example, `DEV_WEBCENTER`.
- `REMAP_TABLESPACE` identifies the source and target tablespace. Remaps all objects selected for import with persistent data in the source tablespace to be created in the target tablespace. For example, `source_tablespace:target_tablespace`.
- `DUMPFILE` contains the data to be imported.

For more information, see "Oracle Data Pump" in the *Oracle Database Utilities* guide.

39.3 Migrating Wiki Documents from Other Wiki Applications

You can migrate wiki content from an external wiki application, such as Confluence, into WebCenter Portal: Spaces using a custom application in combination with the Document Migration Utility. The custom wiki extraction tool extracts the wiki content into an archive format that you can import into a Spaces content repository, using the Document Migration Utility.

To write such a custom wiki extraction tool, you'll need a detailed understanding of the content created in Content Server for a space, space template, wiki documents, and wiki pages, along with a detailed understanding of the Document Migration Utility and the format of its archive. This section describes these formats and processes in the following subsections:

- [Section 39.3.1, "Understanding Document Content in Spaces and Space Templates"](#)
- [Section 39.3.2, "Understanding Wiki Documents and Wiki Pages"](#)
- [Section 39.3.3, "Understanding the Document Migration Utility"](#)
- [Section 39.3.4, "Migrating Data from the Source Wiki Application to Spaces"](#)

39.3.1 Understanding Document Content in Spaces and Space Templates

When the Documents service is enabled in a space or space template, data is created in Content Server.

This section contains the following subsections:

- [Section 39.3.1.1, "Understanding Spaces"](#)
- [Section 39.3.1.2, "Understanding Space Templates"](#)
- [Section 39.3.1.3, "Understanding Folder and File Limitations for a Folder"](#)
- [Section 39.3.1.4, "Understanding Export/Import for Spaces and Space Templates"](#)

39.3.1.1 Understanding Spaces

When a space has the Documents service enabled (either on creation or post creation) a folder is created in Content Server under the root folder containing all the space folders. The root folder is specified in the settings on the primary content repository connection. For more information about connection properties, see [Section 11.2.3.13.2, "Configuring the Content Server Connection for Spaces."](#)

The GUID of the folder created for the space is derived from the internal identifier of the space in Spaces. For example, if the root folder is `WebCenter` and the space `Marketing` is being created, the following data is created in Content Server:

```
Folder Name = Marketing
Folder Path = /WebCenter/Marketing
Folder GUID = 13828FE1-75D8-4A0B-A53B-A76AE78C1AE6
```

When document content (files/folders/wikis, etc.) is added to the space, the artifacts are created inside the space folder in Content Server.

39.3.1.2 Understanding Space Templates

For space templates, the folder is created in the `spacetemplates` folder that resides under the root folder. The GUID of the folder created for the space template will match the internal identifier of the space template in Spaces.

For example, if the root folder is `WebCenter` and the space template `Template1` is being created, the following data is created in Content Server:

```
/WebCenter/spacetemplates/Template1
```

Document content can only be added to a template when the template is created; it cannot be added after the template has been created. When creating a template from a space, if **Documents** is checked on the Content tab of the Create Template dialogue, the document contents in the space are copied to the template.

39.3.1.3 Understanding Folder and File Limitations for a Folder

Content Server has a limit on the number of folders and the number of files that are permitted to be created inside a folder. When the limit of each setting is reached, additional content of that type cannot be added to that folder.

These settings should be large enough to enable users to be able to create a reasonable amount of content, but not so large that they will impair the user interface when rendering that content. Any changes to these settings will only affect new content being added, if you have an existing folder with content larger than these settings, the will not be affected.

To edit the settings for the number of folders and files:

1. Log into Content Server.
2. Go to **Administration > Folder Configuration**.

3. In the Virtual Folder Administration Configuration section, adjust the settings for **Maximum Folders Per Virtual Folder** and **Maximum Content Per Virtual Folder** as appropriate for your environment.

For more information about these settings, see Section A.4.1, "Virtual Folder Administration Configuration Screen" in *Oracle WebCenter Content Application Administrator's Guide for Content Server*.

Note: The root folder containing all the space folders for a WebCenter Portal: Spaces instance bypasses these settings, enabling more space folders to be created than the limit.

39.3.1.4 Understanding Export/Import for Spaces and Space Templates

WebCenter Portal: Spaces provides tools to export and import spaces and space templates. On import, the Documents service is enabled or disabled in the target to match that of the source. If the Documents service is enabled in the source, a folder is created in the target Content Server for the space or space template, and appropriate Content Server permissions are granted to users and groups with access to the space or space template. The GUID of the folder in Content Server for a space or space template will be the same in the source and target Content Server. See [Section 39.3.1, "Understanding Document Content in Spaces and Space Templates"](#) for more information about the folders created in Spaces for spaces and space templates.

Before document content can be migrated from the source to target instances using the Document Migration Utility, the Spaces migration must have completed successfully so that Content Server has folders created for the spaces and space templates that have Documents enabled. For more information about Spaces migration, see [Section 39.1, "Exporting and Importing a Spaces Application for Data Migration."](#)

39.3.2 Understanding Wiki Documents and Wiki Pages

This section describes the format and how wiki documents and wiki pages work in Spaces. For more information about wiki documents and wiki pages in Spaces, see "Working with Wiki Documents" in Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces.

This section contains the following subsections:

- [Section 39.3.2.1, "Understanding Wiki Documents"](#)
- [Section 39.3.2.2, "Understanding Wiki Pages"](#)

39.3.2.1 Understanding Wiki Documents

In WebCenter Portal: Spaces you can create a wiki document using the Documents service. These documents can reside anywhere in the hierarchy of any created folders inside a space. Wiki documents can sit alongside documents of other types, or you could choose to arrange all your wiki documents inside a single folder.

When a wiki document is created in Spaces, an HTML document is created and checked into Content Server. This wiki document contains special metadata values that tell Spaces that the document is a wiki document as opposed to a regular HTML document. These metadata values are:

```
dDocType = Application
dDocFunction = wiki
dOriginalName (document filename) = <wikiName>.htm
```

When you open a document in Spaces with the above metadata, Spaces will know to display it as a wiki document.

39.3.2.2 Understanding Wiki Pages

In WebCenter Portal: Spaces you can create a wiki page by creating a page based on the `wiki` page template. When you navigate to a wiki page you are presented with a wiki document. Depending on the display template of your space, you may see a **Wikis** menu, which you can click to list all the wiki pages in your space. See "Creating a Wiki Document Using the Wiki Page Style" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces* for details on how to create Wiki pages.

When a wiki page is created in Spaces the following artifacts are created in Content Server:

- A folder is created in the folder for the space the wiki page is being created in; the name of the wiki folder is the same name as the wiki page name but with special characters removed.
- A document is created inside the wiki folder with the following metadata:
 - `dDocTitle` = document title (same name as the wiki page name with an extension of `.htm`)
 - `dOriginalName` = the documents filename (same as `dDocTitle`)
 - `dDocFunction` = `wiki`
 - `dDocType` = `Application`
 - `xWCPageID` = the name of the wiki page's JSPX page

This is best illustrated with an example. If the root folder is `WebCenter`, the space in which a wiki page is being created is `Marketing`, and the wiki page being created is `Wiki1`, the following artifacts will be created in Content Server:

- Folder: `/WebCenter/Marketing/Wiki1`
- Document: `/WebCenter/Marketing/Wiki1/Wiki1.htm`
 - `dDocTitle` = `Wiki1.htm`
 - `dOriginalName` = `Wiki1.htm`
 - `dDocFunction` = `'wiki'`
 - `dDocType` = `'Application'`
 - `xWCPageID` = `Wiki1.jspx`

When you navigate to a wiki page the following occurs:

- WebCenter Content is queried for the document in the following location:
`</RootFolder></GroupSpaceFolder></wikiPageName></wikiPageName>.htm`
For example: `/WebCenter/Marketing/Wiki1/Wiki1.htm`
- If the document is found, it is displayed as a wiki document.
- If the document is not found the wiki page will display the contents of the wiki folder.

39.3.3 Understanding the Document Migration Utility

This section provides a detailed description of the inner workings of the utility, and the format of the resulting document migration archive, which you'll need to write a custom wiki extraction tool. The Document Migration Utility exports space and space template documents into an archive that the utility can subsequently use to import the archived documents into the target. For more information about how to use the Document Migration Utility, see [Section 39.1.7.5.2, "Migrating Content Using the Document Migration Utility."](#)

This section contains the following subsections:

- [Section 39.3.3.1, "Understanding the Document Migration Utility's Export Function"](#)
- [Section 39.3.3.2, "Understanding the Document Migration Utility's Import Function"](#)

39.3.3.1 Understanding the Document Migration Utility's Export Function

On export the document content stored in Content Server for the specified spaces and space templates are extracted into a Document Migration Archive. The Document Migration Archive extracts all the contents of a space or space template into its own top-level folder in the archive. The name of this folder is based on the internal GUID of the space or space template folder in Content Server.

The Document Migration Archive will contain a root folder for each space or space template in the export. That is, if you are exporting content from four spaces, the archive will have four root folders. The names of these root folders is based on the internal GUID of the corresponding space or space template folder in Content Server.

In order to have one archive per space or space template, the Document Migration Utility should be called specifying one space/space template at a time and a unique archive name.

Inside each top level folder in the archive is an XML document (`ExportImportData.xml`) that fully describes the data in that root folder (that is, it describes the data exported for that space or space template). It contains all the metadata of the folders and files in the source Content Server that are to be maintained on import. For more information about the format of the archive, see [Section 39.3.3, "Understanding the Document Migration Utility."](#) For more information about the metadata maintained between the source and target, see [Section 39.3.3.2.1, "Understanding How the Document Migration Utility Handles Metadata."](#)

Assuming there are spaces or space templates for which contents are to be exported, the following occurs during export:

- A temporary directory is created.
- For each space or space template:
 - a directory is created in the temporary directory with its name being the GUID of the corresponding folder in Content Server
 - an `ExportImportData.xml` document is created inside that new directory
 - Content Server is queried for the contents of the space/space template
 - If there are contents, they are read and information about the folders/documents are written to the `ExportImportData.xml` document and the files are downloaded into the temporary directory

- If there are contents, they are read and information about the folders and documents are written to the `ExportImportData.xml` document. The actual files are downloaded into the directory maintaining the folder hierarchy as in the Content Server. For example, if in the Content Server the document `doc1.doc` is in folder `Folder1` the document will be added to the root folder under `Folder1` as shown below.

```
<tmpDir>/<spaceFolder>/Folder1/doc1.doc
```

- After all contents have been extracted, the entire contents of the temporary directory are zipped up into the Document Migration Archive.

39.3.3.2 Understanding the Document Migration Utility's Import Function

Before the Document Migration Utility is run, the Spaces migration must have completed successfully to ensure the space and/or space templates have been created correctly in the target Content Server. If these folders do not exist in Content Server the import of document content will fail. For more information about migrating Space, see [Section 39.1, "Exporting and Importing a Spaces Application for Data Migration."](#)

Note: You cannot simply create a space or space template in the target with the same name as in the source and expect it to work. If you do this, the folder in Content Server will have the same name as in the source but with a different GUID. It is this folder GUID that is used to tie the space in Spaces with the folder in Content Server as well as what is used to synchronize the data in the export archive with the target folder in the target Content Server.

On import, the Document Migration Archive is read and for each space or space template's data the content is recreated in the corresponding space or space template's folder in the target Content Server. The names of the top level folders in the archive are used to synchronize with the space or space template folder in the target Content Server instance. If the space or space template folders in the target Content Server already contain contents, by default the contents are deleted before the import process begins.

Note: the default behavior can be overwritten by specifying the `CheckExistingContents` property (values are `true` or `false`) in the properties file when running the Document Migration Utility specifying all the properties in a file. When set to `false`, the default behavior is overridden such that the target folder is not checked for any existing content and any existing content is not deleted. Care should be taken with having this setting as `false`; if there is any content in the target with the same Content ID or any content in the same folder with the same filename, the import will fail.

The XML document (`ExportImportData.xml`) located inside each top level folder is used to drive the import. This document describes the hierarchy of files and folders to recreate in the target Content Server. It also contains the metadata to be used when creating the artifacts and for documents it contains the path to the native file in the archive to use in the upload. For more information about the format of the archive, see [Section 39.3.3, "Understanding the Document Migration Utility."](#)

On import, the following happens:

- The Document Migration Archive is unzipped into a temporary directory
- For each folder at the root of the archive (which represent a space or space template):
 - The corresponding folder is obtained from the target Content Server instance (using the folder name that is the GUID of the folder in Content Server)
 - The `ExportImportData.xml` document is read
 - For each folder or file described in the `ExportImportData.xml` the contents are recreated in the target instance

The attributes in the `ExportImportData.xml` document for the folders and files are used as metadata for the contents being created and the files are uploaded from the corresponding location in the archive.
- At the end of a successful import, this temporary directory is deleted. If the import fails before completion, this temporary directory will remain.

39.3.3.2.1 Understanding How the Document Migration Utility Handles Metadata

The Document Migration Utility will maintain as much metadata as possible between the source and target. Most internal metadata (such as IDs), however, are not maintained. The following metadata is not included in the export set:

- Any date metadata, such as the creation date (for example, `dCreateDate`, `dReleaseDate`, `dDocLastModifiedDate`)
- For a document:
 - No internal identifiers for the document revisions or renditions (for example, `dID`, `dDoc`). Note that the content ID, `dDocName`, is included
 - The ID of the folder in which the document resides (for example, `xCollectionID`)
 - No Web-viewable renditions, as these will be recreated when the document is checked into the target
 - No information about the actual file (for example, its file type or mimetype) as these will get set when document is checked into the target
 - No status information, such as checked out, released state as these are irrelevant when creating the document in the target (for example, `dIsCheckedOut`, `dReleaseState`)
- For a folder:
 - No internal identifiers or paths such as the parent folder ID, or its own path (for example, `hasCollectionID`, `dCollectionID`, `dCollectionGUID`, `hasCollectionPath`, `dCollectionPath`)
- Storage rule, as this is dependent on the configuration of the target Content Server
- Security group or other security permissions, as these will get set when the content is created in the target (for example, `dSecurityGroup`, `dRead`, `canReadCollection`)

Metadata that is maintained:

- Names of artifacts, such as folder name or document title (for example, `dCollectionName`, `dDocTitle`)
- Username of person who created the content and modified it (for example, `dCollectionOwner`, `dDocOwner`)

- Wiki metadata, such as `dDocFunction`, `dDocType`, `xWCPageID`
- For a document:
 - The name of the file to upload for the document (`dOriginalName`)
 - The content ID (`dDocName`)

If at the time of import a content item already exists in the target Content Server with the same content ID, import will fail. When rerunning an import with the property `CheckExistingContents=false` set, ensure that the target folder does not already contain the contents from the archive being imported to avoid a content ID error.

- Custom metadata (for example, `myCustomInteger`).

39.3.3.2.2 Document Migration Archive

The Document Migration Utility creates a single archive when exporting content from a source Content Server. The archive is used when running the Document Migration Utility to import the data into the target environment. The Document Migration archive has a specific layout and if an archive does not match this layout, the Document Migration Utility import will fail.

Archive format

The following describes the layout of the Document Migration Archive.

At the top level of the archive is a folder for each space/space template that has had their data exported.

- If a single space/space template has been exported there will only be one root folder, if multiple spaces/space templates have been exported there will be multiple root folders.
- The root folder names are the same as the internal GUID of the corresponding folder in Content Server (for example, `13828FE1-75D8-4A0B-A53B-A76AE78C1AE6`)

In each top level folder is an `ExportImportData.xml` document that describes the hierarchy of files and folders to recreate in the target Content Server for that space or space template. This document contains the metadata to be used when creating the artifacts (internal metadata, such as `xCollectionID`, `isreadonly`, `xStorageRule`, will not be included). For documents, it contains the path to the native file in the archive to use in the upload.

In each top-level space and space template folder are the exported documents. The layout of the documents inside the top-level folder mimics the layout in the source space and space template in the source Content Server. For example, if document `doc1.doc` resides in `folder1`, the top-level folder in the archive will contain a folder `folder1` in which `doc1.doc` resides. The documents file/folder structure in the top-level folder must match the hierarchy described in the `ExportImportData.xml` so that the import code can find the native file for the documents described in that document uploading the document into the target. Empty folders in the space or space template folder in the source will not be in the archive. However, these folders are still described in the `ExportImportData.xml` document in order for them to be recreated in the target.

In a simplified overview, this would look like:

- Space1 top level folder:
 - `ExportImportData.xml`

- <Space1's documents arranged in the same folder hierarchy as in the source>
- Space2 top level folder:
 - ExportImportData.xml
 - <Space2's documents arranged in the same folder hierarchy as in the source>

Understanding the ExportImportData.xml Document

The XSD for the ExportImportData.xml document is shown below.

XSD for ExportImportData.xml:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">

<xs:element name="groupspace-folder" type="FolderType" />

<!-- 'folders' must contain 1 or more 'folder' child elements -->
<xs:complexType name="FoldersType">
  <xs:sequence>
    <xs:element name="folder" type="FolderType"
      minOccurs="1" maxOccurs="unbounded" />
  </xs:sequence>
</xs:complexType>

<!-- 'documents' must contain 1 or more 'document' elements -->
<xs:complexType name="DocumentsType">
  <xs:sequence>
    <xs:element name="document" type="DocumentType"
      minOccurs="1" maxOccurs="unbounded" />
  </xs:sequence>
</xs:complexType>

<!-- 'attributes' must have 1 or more 'attribute' child elements -->
<xs:complexType name="AttributesType">
  <xs:sequence>
    <xs:element name="attribute" type="AttributeType"
      minOccurs="1" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>

<!-- 'folder' has to have 1 and only 1 'attributes' child element
  0 or 1 'folders' child element, 0 or 1 'documents' child element -->
<xs:complexType name="FolderType">
  <xs:sequence>
    <xs:element name="attributes" type="AttributesType"
      minOccurs="1" maxOccurs="1" />
    <xs:element name="folders" type="FoldersType"
      minOccurs="0" maxOccurs="1" />
    <xs:element name="documents" type="DocumentsType"
      minOccurs="0" maxOccurs="1" />
  </xs:sequence>
</xs:complexType>

<!-- 'document' has to have : 1 and only 1 'attributes' child element
  and nothing else -->
<xs:complexType name="DocumentType">
  <xs:sequence>
    <xs:element name="attributes" type="AttributesType"
      minOccurs="1" maxOccurs="1" />
  </xs:sequence>
</xs:complexType>
```

```
</xs:sequence>
</xs:complexType>

<!-- 'attribute' element has to have a 'name' and 'value' attributes -->
<xs:complexType name="AttributeType">
  <xs:attribute name="name" type="xs:string" use="required" />
  <xs:attribute name="value" type="xs:string" use="required" />
</xs:complexType>

</xs:schema>
```

Where:

- **<groupspace-folder>** is the root tag that represents the space or space template folder.
This tag contains the `<attributes>` tag, which in turn contains a number of attributes about the root folder and export data. These attributes are for information purposes only; they are *not* used in the import.
- **<attributes>** is used to group all the attributes of the document or folder.
This tag must contain one or more `<attribute>` tags. No other child tags are permitted.
- **<attribute>** contains the metadata for a folder or document.
This tag has two attributes:
 - name - the Content Server metadata name
 - value - the value of the metadataNo child tags are permitted.
- **<folders>** is used to group all the folders in the current folder
This tag must contain 1 or more `<folder>` tags. No other child tags are permitted.
- **<folder>** is used to indicate a child folder.
This tag must have the `<attributes>` tag. If the folder has child folders, it will have the `<folders>` tag. If the folder has child documents, it will have the `<documents>` tag.
- **<documents>** is used to group all the documents in the current folder.
This tag must contain one or more `<document>` tags. No other child tags are permitted.
- **<document>** is used to indicate a document in the current folder.
This tag must have the `<attributes>` tag. No other child tags are permitted.

Annotated example:

The following annotated example shows a partially complete `ExportImportData.xml` document. Note that the example contains blank lines and XML comments that should not exist in a real `ExportImportData.xml` document.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<groupspace-folder>

  <attributes>
    <!-- Contains a set of attributes of the main space folder -->
    <attribute name="export-date" value="2011-07-22 13:02:29"/>
```



```

</attributes>

<folders> <!-- only present if the space contains any child folders -->
  <folder> <!-- a 'folder' tag exists for each child folder -->
    <attributes>
      <!-- contains the set of folder attributes, examples below -->
      <attribute value="F1" name="dCollectionName"/>
    </attributes>
    <!-- a 'folder' tag will contain the 'folders' tag if this folder
      contains child folders, i.e. if 'F1' has child folders -->
    <folders>
      <folder>
        <!-- attribute tags, child folders, child documents etc -->
      </folder>
    </folders> <!-- closing tag for all the folders in the
      current folder -->
    <!-- a 'folder' tag will contain the 'documents' tag if this folder
      contains documents, i.e. if 'F1' has documents at its root -->
    <documents>
      <document>
        <!-- attributes tags, see below -->
      </document>
    </documents> <!-- closing tag for all the documents in the
      current folder -->
  </folder> <!-- closing tag for folder 'F1' -->
</folders> <!-- closing tag for all the folders in the space root -->

<documents> <!-- only present if the folder contains any documents
  in the root folder -->
  <document> <!-- a 'document' tag exists for each document in the
    folder -->
    <attributes>
      <!-- contains the set of document attributes, examples below -->
      <attribute name="dDocTitle" value="Doc1"/>
      <attribute name="xForceFolderSecurity" value="TRUE"/>
      <attribute name="xSecurityClearanceLevel" value="public"/>
    </attributes>
    <document> <!-- closing tag for document 'Doc1' -->
  </documents><!-- closing tag for all the documents in the space root -->

</groupspace-folder>

```

Building the ExportImportData.xml Document

The following shows pseudo code for how the XML document is built:

- query Content Server for the space's folder information
 - create a 'group-space-folder' node
 - create an 'attributes' node
 - for each of the three attributes we want to maintain (folder name, path and GUID)
 - create an 'attribute' node with name and value
 - add that 'attribute' node to the 'attributes' node
 - add that 'attributes' node to the 'group-space-folder' node
- query Content Server for the contents of the space root folder
 - * If there are child folders
 - Create a 'folders' node
 - For each child folder
 - create a 'folder' node
 - create an 'attributes' node

- for each folder metadata we want to maintain
 - create an 'attribute' node with name and value
 - add that 'attribute' node to the 'attributes' node
- add the 'attributes' node to the 'folder' node
- query Content Server for the contents of this current folder
 - go to * and repeat traversing folders which reside in this current folder
 - go to # and repeat for documents which reside in this current folder
 - add the 'folder' node to the 'folders' node
- add the 'folders' node to the parent node (which will either be a 'folder' node or the 'group-space-folder' node)
- # If there are documents in this current folder
 - create a 'documents' node
 - for each document
 - create a 'document' node
 - create an 'attributes' node
 - for each metadata we want to maintain
 - create an 'attribute' node with name and value
 - add that 'attribute' node to the 'attributes' node
 - add the 'attributes' node to the 'document' node
 - add that 'document' node to the 'documents' node
 - add the 'documents' node to the 'folder' node
- use jaxb to write the whole data to an xml file

Document Migration Archive Example

Below is an example of the archive format for a set of sample data and a sample `ExportImportData.xml` document for one of the spaces in the example.

WebCenter Data

In the example below, two spaces (Marketing and Sales) have been created in Spaces. In the Marketing space two wiki pages have been created: `MarketingWiki` and `Tradeshows`. The Marketing space has also had two folders created (Branding and Presentations), the latter of which contains subfolders with a PowerPoint document and a wiki document. The Sales space has no wiki pages, but does contain three folders with some contents.

- Marketing
 - Marketing space contains the Content Server folder GUID=`29A4E019-7AE7-46A1-823B-AF16A313BBEF`
 - MarketingWiki
 - * `MarketingWiki.htm` with the following metadata:


```
dOriginalName="MarketingWiki.htm"
dDocTitle="MarketingWiki.htm"
dDocFunction="wiki"
dDocType="Application"
xWCPageID="Page2.jspx"
```
 - Presentations
 - * Branding
 - `ProductBranding.pptx`
 - * `Presentation Dates.htm` with the following metadata:

(Note that here the wiki document is created inside a folder in a space,

rather than being created when a wiki page is created as for MarketingWiki.htm above)

```
dOriginalName=" Presentation Dates.htm"
```

```
dDocTitle="Presentation Dates"
```

```
dDocFunction="wiki"
```

```
dDocType="Application"
```

```
xWCPageID = not set (as the wiki was not created when creating a wiki page)
```

```
* ProjectedDesigns.pptx
```

- Products
- TradeShows

```
* TradeShows.htm with the following metadata:
```

```
dOriginalName=" TradeShows.htm"
```

```
dDocTitle=" TradeShows.htm"
```

```
dDocFunction="wiki"
```

```
dDocType="Application"
```

```
xWCPageID=" Page4.jspx"
```

- Sales

```
WebCenter Content folder GUID =
629BFEBD-4E83-4DCA-895A-C72E5192FBFD
```

- DecConference
 - * GuestSpeakers.doc
- SalesConference
 - * Attendees.doc
 - * TalkSchedules.doc
- BudgetForcasts.doc

Archive Contents

- 29A4E019-7AE7-46A1-823B-AF16A313BBEF (contains Marketing space contents)
 - MarketingWiki
 - * MarketingWiki.htm
 - Presentations
 - * Branding (ProductBranding.pptx)
 - * ProjectedDesigns.pptx
 - * Presentation Dates.htm
 - Tradeshow
 - * TradeShows.htm
 - ExportImportData.xml
 - 2001Plans.doc
- 629BFEBD-4E83-4DCA-895A-C72E5192FBFD (contains Sales space contents)
 - DecConference

- * GuestSpeakers.doc
- SalesConference
 - * Attendees.doc
 - * TalkSchedules.doc
- ExportImportData.xml
- BudgetForcasts.doc

Note: There is no Products folder under the Marketing space's root folder as this folder did not contain any documents.

ExportImportData.xml for the Marketing space

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<groupspace-folder>
  <attributes>
    <attribute value="2011-10-27 15:50:18" name="export-date" />
    <attribute value="/WebCenter0711/Marketing/" name="group-space-path" />
    <attribute value="Marketing" name="group-space-name" />
    <attribute value="29A4E019-7AE7-46A1-823B-AF16A313BBEF"
      name="group-space-guid" />
  </attributes>
  <folders>
    <folder>
      <attributes>
        <attribute value="TRUE" name="xForceFolderSecurity" />
        <attribute value="weblogic" name="dCollectionCreator" />
        <attribute value="MarketingWiki" name="dCollectionName" />
        <attribute value="0" name="isLink" />
        <attribute value="Page2.jspx" name="xWCPageId" />
        <attribute value="sysadmin" name="dCollectionOwner" />
        <attribute value="weblogic" name="dCollectionModifier" />
        <attribute value="1" name="dCollectionEnabled" />
      </attributes>
      <documents>
        <document>
          <attributes>
            <attribute value="TRUE" name="xForceFolderSecurity" />
            <attribute value="Page2.jspx" name="xWCPageId" />
            <attribute value="wiki" name="dDocFunction" />
            <attribute value="Application" name="dDocType" />
            <attribute value="0" name="ishidden" />
            <attribute value="weblogic" name="dDocOwner" />
            <attribute value="MarketingWiki.htm" name="dOriginalName" />
            <attribute value="MarketingWiki.htm" name="dDocTitle" />
            <attribute value="FALSE" name="xInhibitUpdate" />
            <attribute value="0" name="isreadonly" />
            <attribute value="0" name="CustomInteger" />
            <attribute value="weblogic" name="dDocCreator" />
            <attribute value="weblogic" name="dDocAuthor" />
            <attribute value="OWCSVR01USORAC012754" name="dDocName" />
            <attribute value="1" name="dRevisionID" />
            <attribute value="weblogic" name="dDocLastModifier" />
          </attributes>
        </document>
      </documents>
    </folder>
  </folders>
</groupspace-folder>
```

```

</folder>
  <attributes>
    <attribute value="TRUE" name="xForceFolderSecurity" />
    <attribute value="weblogic" name="dCollectionCreator" />
    <attribute value="Presentations" name="dCollectionName" />
    <attribute value="0" name="isLink" />
    <attribute value="sysadmin" name="dCollectionOwner" />
    <attribute value="weblogic" name="dCollectionModifier" />
    <attribute value="1" name="dCollectionEnabled" />
  </attributes>
</folders>
<folder>
  <attributes>
    <attribute value="TRUE" name="xForceFolderSecurity" />
    <attribute value="weblogic" name="dCollectionCreator" />
    <attribute value="Branding" name="dCollectionName" />
    <attribute value="0" name="isLink" />
    <attribute value="sysadmin" name="dCollectionOwner" />
    <attribute value="weblogic" name="dCollectionModifier" />
    <attribute value="1" name="dCollectionEnabled" />
  </attributes>
  <documents>
    <document>
      <attributes>
        <attribute value="TRUE" name="xForceFolderSecurity" />
        <attribute value="Document" name="dDocType" />
        <attribute value="weblogic" name="dDocOwner" />
        <attribute value="0" name="ishidden" />
        <attribute value="ProductBranding.pptx" name="dDocTitle" />
        <attribute value="ProductBranding.pptx"
          name="dOriginalName" />
        <attribute value="FALSE" name="xInhibitUpdate" />
        <attribute value="0" name="isreadonly" />
        <attribute value="0" name="CustomInteger" />
        <attribute value="weblogic" name="dDocCreator" />
        <attribute value="weblogic" name="dDocAuthor" />
        <attribute value="OWCSVR01USORAC012748" name="dDocName" />
        <attribute value="1" name="dRevisionID" />
        <attribute value="weblogic" name="dDocLastModifier" />
      </attributes>
    </document>
  </documents>
</folder>
</folders>
<documents>
  <document>
    <attributes>
      <attribute value="TRUE" name="xForceFolderSecurity" />
      <attribute value="wiki" name="dDocFunction" />
      <attribute value="Application" name="dDocType" />
      <attribute value="0" name="ishidden" />
      <attribute value="weblogic" name="dDocOwner" />
      <attribute value="Presentation Dates" name="dDocTitle" />
      <attribute value="Presentation Dates.htm"
        name="dOriginalName" />
      <attribute value="FALSE" name="xInhibitUpdate" />
      <attribute value="0" name="isreadonly" />
      <attribute value="0" name="CustomInteger" />
      <attribute value="weblogic" name="dDocCreator" />
      <attribute value="weblogic" name="dDocAuthor" />
    </attributes>
  </document>
</documents>

```

```

        <attribute value="OWCSVR01USORAC012758" name="dDocName" />
        <attribute value="1" name="dRevisionID" />
        <attribute value="weblogic" name="dDocLastModifier" />
    </attributes>
</document>
<document>
    <attributes>
        <attribute value="TRUE" name="xForceFolderSecurity" />
        <attribute value="Document" name="dDocType" />
        <attribute value="weblogic" name="dDocOwner" />
        <attribute value="0" name="ishidden" />
        <attribute value="ProjectedDesigns.pptx" name="dDocTitle" />
        <attribute value="ProjectedDesigns.pptx"
            name="dOriginalName" />
        <attribute value="FALSE" name="xInhibitUpdate" />
        <attribute value="0" name="isreadonly" />
        <attribute value="0" name="CustomInteger" />
        <attribute value="weblogic" name="dDocCreator" />
        <attribute value="weblogic" name="dDocAuthor" />
        <attribute value="OWCSVR01USORAC012747" name="dDocName" />
        <attribute value="1" name="dRevisionID" />
        <attribute value="weblogic" name="dDocLastModifier" />
    </attributes>
</document>
</documents>
</folder>
<folder>
    <attributes>
        <attribute value="TRUE" name="xForceFolderSecurity" />
        <attribute value="weblogic" name="dCollectionCreator" />
        <attribute value="Products" name="dCollectionName" />
        <attribute value="0" name="isLink" />
        <attribute value="sysadmin" name="dCollectionOwner" />
        <attribute value="weblogic" name="dCollectionModifier" />
        <attribute value="1" name="dCollectionEnabled" />
    </attributes>
</folder>
<folder>
    <attributes>
        <attribute value="TRUE" name="xForceFolderSecurity" />
        <attribute value="weblogic" name="dCollectionCreator" />
        <attribute value="TradeShows" name="dCollectionName" />
        <attribute value="0" name="isLink" />
        <attribute value="Page4.jspx" name="xWCPageId" />
        <attribute value="sysadmin" name="dCollectionOwner" />
        <attribute value="weblogic" name="dCollectionModifier" />
        <attribute value="1" name="dCollectionEnabled" />
    </attributes>
</documents>
<document>
    <attributes>
        <attribute value="TRUE" name="xForceFolderSecurity" />
        <attribute value="Page4.jspx" name="xWCPageId" />
        <attribute value="wiki" name="dDocFunction" />
        <attribute value="Application" name="dDocType" />
        <attribute value="0" name="ishidden" />
        <attribute value="weblogic" name="dDocOwner" />
        <attribute value="TradeShows.htm" name="dOriginalName" />
        <attribute value="TradeShows.htm" name="dDocTitle" />
        <attribute value="FALSE" name="xInhibitUpdate" />
    </attributes>
</document>
</documents>

```

```

        <attribute value="0" name="isreadonly" />
        <attribute value="0" name="CustomInteger" />
        <attribute value="weblogic" name="dDocCreator" />
        <attribute value="weblogic" name="dDocAuthor" />
        <attribute value="OWCSVR01USORAC012756" name="dDocName" />
        <attribute value="1" name="dRevisionID" />
        <attribute value="weblogic" name="dDocLastModifier" />
    </attributes>
</document>
</documents>
</folder>
</folders>
<documents>
  <document>
    <attributes>
      <attribute value="TRUE" name="xForceFolderSecurity" />
      <attribute value="Document" name="dDocType" />
      <attribute value="weblogic" name="dDocOwner" />
      <attribute value="0" name="ishidden" />
      <attribute value="2011Plans.doc" name="dDocTitle" />
      <attribute value="2011Plans.doc" name="dOriginalName" />
      <attribute value="FALSE" name="xInhibitUpdate" />
      <attribute value="0" name="isreadonly" />
      <attribute value="0" name="CustomInteger" />
      <attribute value="weblogic" name="dDocCreator" />
      <attribute value="weblogic" name="dDocAuthor" />
      <attribute value="OWCSVR01USORAC012746" name="dDocName" />
      <attribute value="1" name="dRevisionID" />
      <attribute value="weblogic" name="dDocLastModifier" />
    </attributes>
  </document>
</documents>
</groupspace-folder>

```

39.3.4 Migrating Data from the Source Wiki Application to Spaces

To migrate content from an existing wiki application to WebCenter Portal: Spaces, perform the following steps:

1. Prepare Spaces for import of the wiki content.
2. Write and run a 'Custom Wiki Extraction Tool' to extract content from the Wiki application into an archive matching the precise format expected for use the Document Migration Utility.
3. Use the Document Migration Utility to import the archive into Content Server.
4. Create any wiki pages in Spaces to tie up with the content in Content Server.

These steps are described in more detail in the following sections:

- [Section 39.3.4.1, "Preparing WebCenter Portal: Spaces for Importing Wiki Content"](#)
- [Section 39.3.4.2, "Writing and Running a Custom Wiki Extraction Tool to Extract Content from the Wiki Application"](#)
- [Section 39.3.4.3, "Using the Document Migration Utility to Import the Archive into the Target Space"](#)
- [Section 39.3.4.4, "Creating Wiki Pages in Spaces for the Content in Content Server"](#)

39.3.4.1 Preparing WebCenter Portal: Spaces for Importing Wiki Content

On provisioning the Documents service in a space or space template, a folder is created in Content Server for that space or space template. The GUIDs of these folders must be determined in order to construct the archive to be used with the Document Migration Utility. The folder GUIDs can be determined by following steps below:

1. Decide if you want to import all the wiki content into a single space or multiple spaces.
2. Log into the Spaces application and create the spaces, taking note of the internal name of the group spaces.

Ensure you are using a template which has the Documents service, otherwise you will have to provision Documents service and setup the role permissions after space creation.

3. Log into Content Server.
4. Ensure that the user's layout is **Top Menus**:
 - a. Click the user's name to display the user's Profile page.
 - b. Under **User Personalization Settings** check that **Layout** is set to Top Menu.
5. For each space in which wiki content is to be imported, determine the folder GUID:

- a. Click **Browse Content**.
- b. Click on the root folder for the Spaces instance.

This is the same as the **Root Folder** setting in the Content Server connection.
- c. Click the folder for the space.

The folder name will be the same as the space's internal name.
- d. Click **Info** on the toolbar to display the folder information.
- e. Add `IsSoap=1` to the URL.
- f. Search for the string `dCollectionGUID`. For example:

```
<idc:field  
name="dCollectionGUID">05573322-E895-EDA3-8A83-07CF39CBDE0  
5</idc:field>
```

6. Keep a note of the space folder name and its GUID as the GUID is needed when building the archive in the next step.

39.3.4.2 Writing and Running a Custom Wiki Extraction Tool to Extract Content from the Wiki Application

To extract content from the source wiki application into an archive suitable for use with the Document Migration Utility, you'll need to write a custom application. For information about the format of the archive, see [Section 39.3.3, "Understanding the Document Migration Utility."](#)

The custom wiki extraction tool must perform the following steps:

1. Extract and arrange the wiki content.

Create a temporary directory and extract the wiki content from the source wiki application into it and arrange in the file system as it is to appear in Spaces.
2. Clean up the source HTML of wiki documents.

For each wiki document, edit the HTML to remove application-specific HTML tags.

3. Re-write the URLs.

For each wiki document, replace the existing URLs to content in the source wiki application to the URLs of the same artifacts that will be imported into Spaces.

4. Build the `ExportImportData.xml` documents.

For each root folder build the `ExportImportData.xml` document which describes the data in the export set and is used to drive the import

5. Build the archive file.

Create an archive of the manipulated wiki content that can be used to import the wiki content into Spaces.

Each of these steps is described more fully in the following sections:

- [Section 39.3.4.2.1, "Extracting and Arranging the Wiki Content"](#)
- [Section 39.3.4.2.2, "Cleaning Up the Source HTML of Wiki Documents"](#)
- [Section 39.3.4.2.3, "Rewriting the URLs"](#)
- [Section 39.3.4.2.4, "Building the ExportImportData.xml Documents"](#)
- [Section 39.3.4.2.5, "Building the Archive File"](#)

39.3.4.2.1 Extracting and Arranging the Wiki Content The wiki documents in the source application need to be extracted into a temporary directory on the file system and then arranged such that the file system mimics how the content is to be laid out in the target Spaces instance. If all the wiki documents are to be imported into a single space, all of the content should be laid out under a single root folder named with the GUID of the corresponding space folder in Content Server. If the wiki documents are to be imported into multiple spaces, the content should be laid out under multiple root folders, each named with the GUID of their corresponding folder in Content Server. For more information on determining the GUID of a space folder in Content Server, see [Section 39.3.4.1, "Preparing WebCenter Portal: Spaces for Importing Wiki Content."](#)

Note that when arranging the wiki content on the file system, you should consider how that content will be used in Spaces. For example:

- If wiki pages are to be created, then the wiki document for that wiki page must be located under a folder of the same name. For more information about wiki pages, see [Section 39.3.2, "Understanding Wiki Documents and Wiki Pages."](#)
- When a folder contains a large number of contents, the rendering of that folder's contents could be impaired.
- Content Server has two settings that limit the number of folders and the number of files which can reside in a folder. When arranging your wiki content, ensure that a folder does not contain more folders than the folder limit setting or more documents than the document limit setting. For more information about folder and file limitations within a space, see [Section 39.3.1.3, "Understanding Folder and File Limitations for a Folder."](#)

To create extracted wiki content, perform the following tasks:

1. Create root folders for each space into which you will be importing the wiki documents, name the folders based on the GUID of the corresponding space folder in Content Server.

2. For wiki documents for which wiki pages will be created in WebCenter Portal: Spaces after import:
 - a. Create a wiki folder with the same name as the wiki document.
 - b. Place the wiki document in this folder.
 - c. Place any other documents in this folder, if required.
 - d. If there are related images and/or documents, add them to this wiki folder as well.
3. For any other wiki documents, create the folder hierarchy that will contain the documents.

Example:

Space S1's folder in Content Server has a GUID of 21SD15F13B8_141D_421B_AD0e_BC54B6F16893. After import, the MarketingWiki and Tradeshows wiki pages will be created and it is expected these wiki pages will show the MarketingWiki.htm and Tradeshows.htm wiki documents.

The following shows the organized structure of the extracted wiki documents and artifacts:

```
21SD15F13B8_141D_421B_AD0e_BC54B6F16893 (Root space folder)
  Home.htm (Wiki document)
  MarketingWiki (Folder)
    MarketingWiki.htm (Wiki document)
  Branding (Folder)
    Presentation Dates.htm (Wiki document)
    Presentations (Folder)
  ProductBranding.pptx (File)
  ProjectedDesigns.pptx (File)
  Tradeshows (Folder)
    TradeShows.htm (Wiki document)
  Images (Folder)
    Image.jpg (Image)
```

39.3.4.2.2 Cleaning Up the Source HTML of Wiki Documents In WebCenter Portal: Spaces, the wiki editor will remove any HTML tags when the wiki page is being edited. Therefore it is advisable to remove any such HTML tags in the wiki documents prior to importing them into WebCenter Portal: Spaces to avoid any confusion of tags being removed when editing a wiki document after import. The following tags can be safely removed:

```
<html>, </html>
<head>, </head>
<meta>, </meta>
<title>, </title>
<body>, </body>
<tbody>, </tbody>
<thead>, </thead>
<tfoot>, </tfoot>
<script>, </script>
<link>, </link>
```

39.3.4.2.3 Rewriting the URLs Wiki pages in the source wiki application may contain URLs referencing artifacts in within the source wiki application, such as links for embedded images or to other wiki page or documents. These artifacts will be migrated

to the target Spaces instance and these links will need to be updated to reference the new artifact locations in the target Spaces instance.

The following types of URLs in the extracted wiki pages need to be changed to reference the URLs of the same artifacts in Spaces:

- Links to other Wiki pages
- Links to embedded images
- Links to documents

Follow the steps below to rewrite the URLs in the wiki documents:

1. Define attributes for the target Spaces instance that will be used in the URL replacement in step 3.
 - **WC_BASE_URL:** WebCenter instance base URL
Example: WC_BASE_URL=https://webcenter.example.com
 - **UCM_ID:** The name of the connection in Spaces to the Content Server
Example: UCM_ID=dev_ucm
 - **SPACE_GUID:** The GUID of the space in Spaces where the content resides
Example:
SPACE_GUID=s21sd15f13b8_141d_421b_ad0e_bc54b6f16893
For more information about determining the GUID, see [Section 39.3.4.1, "Preparing WebCenter Portal: Spaces for Importing Wiki Content."](#)
2. For each content item, define the item attributes that will be used in the URL replacement in step 3.
 - **FILE_NAME:** File name of the content item
Example: FILE_NAME=Home.htm
 - **FILE_ID:** Unique Content Server content ID
Example: MARKETINGSPEACE1001

Note that the FILE_ID must be unique across the entire Content Server instance. A suggested value is the name of the space which the wiki documents are going to be imported into (with no space in the name) post-fixed with a unique number (in the example above, the space name was Marketing Space).

3. Rewrite the URLs using the defined attributes as shown below:

Embedded images

- New URL format:


```
IMG_REPLACE=img alt="FILE_NAME"
resourceid="UCM_ID#dDocName:FILE_ID"
src="WC_BASE_URL/webcenter/content/conn/UCM_ID/uuid/dDocName%3aFILE_ID"
```
- Example:
 - Source URL:


```

```
 - WebCenter URL:

```

```

Wiki pages

- New URL format:

```
URL_REPLACE=WC_BASE_URL/webcenter/faces/owResource.jspx?z=  
oracle.webcenter.doclib%21SPACE_GUID%21UCM_ID%2523dDocName  
%253AFILE_ID%21%21FILE_NAME
```

- Example:

- Source URL:

```
<a href="Home.htm">Home</a>
```

- WebCenter URL:

```
<a href="http://webcenter.example.com/web-  
center/faces/owResource.jspx?z=oracle.web-  
center.doclib%21sd15f13b8_141d_421b_ad0e_bc54b6f16893%2  
1dev-ucm%2523dDocName%253AWSIMPORT25%21%21Home.htm>Home  
</a>
```

Links to documents

- New URL format:

```
DOCUMENT_REPLACE=WC_BASE_URL/webcenter/content/conn/UCM_ID  
/uuid/dDocName%3aFILE_ID
```

- Example:

- Source URL:

```
<a href="MarketingWiki/Presentations/ProductBrand-  
ing.pptx"> Download Product Branding Presentation</a>
```

- WebCenter URL:

```
<a href="http://webcenter.example.com/webcenter/con-  
tent/dev-ucm/uuid/dDocName%3aWSIMPORT7"> Download Prod-  
uct Branding Presentation</a>
```

39.3.4.2.4 Building the ExportImportData.xml Documents In each root folder containing the contents to be imported an `ExportImportData.xml` document needs to be created. The `ExportImportData.xml` document describes the contents of the root folder and is used to drive the import when importing the content into Spaces using the Document Migration Utility. For more information about the Document Migration Utility and the `ExportImportData.xml` document, see [Section 39.3.3, "Understanding the Document Migration Utility."](#)

Any metadata to be created with the document on import must be specified in the `ExportImportData.xml` document. In Spaces, wiki documents are stored as HTML documents but have extra metadata to identify them as wiki documents rather than normal HTML documents. Ensure the `ExportImportData.xml` document has this metadata specified for all wiki documents in the extracted contents. For more information about the metadata required for wiki document, see [Section 39.3.2, "Understanding Wiki Documents and Wiki Pages."](#)

Note: A content ID (dDocName) is automatically generated by Content Server when a document is checked in without one being specified. If you wish your documents to have fixed content IDs, include the dDocName metadata with the document metadata in the ExportImportData.xml document. The dDocName must be unique across the whole Content Server or document check in will fail. A suggestion is to chose your own prefix for the content ID and append numbers incrementally to the end.

The ExportImportData.xml document can be generated manually for each root folder. Alternatively, you can write a custom script to traverse through the root folder contents and generate the document.

It is imperative for the structure of the contents on the file system is detailed in ExportImportData.xml document correctly. If there is a mismatch between the hierarchy of contents described in the ExportImportData.xml document and the file system, the import into the space folder in the target Content Server will fail.

Example:

In this example a custom script named convert_program traverses through a root folder called 21SD15F13B8_141D_421B_AD0e_BC54B6F16893 and creates an ExportImportData.xml document in the current working directory detailing the contents of the folder.

```
cd 21SD15F13B8_141D_421B_AD0e_BC54B6F16893
run convert_program
```

39.3.4.2.5 Building the Archive File Create an archive of the extracted and manipulated wiki documents by zipping up the root space folders. The zip archive must have the root folders inside the archive rather than just the contents of the root folders. One zip file can contain multiple root folders for different spaces, or you can create one zip file for each root folder.

Example:

In the following example, wiki documents have been extracted and manipulated in a folder called 21SD15F13B8_141D_421B_AD0e_BC54B6F16893 in the folder /scratch/wikiexports and the archive to create is wsimport.zip.

```
cd /scratch/wikiexports
zip -r wsimport.zip 21SD15F13B8_141D_421B_AD0e_BC54B6F16893/
```

Note: Ensure that the archive does not exist prior to zipping up the folder contents as some zip tools will add content to the specified archive if it already exists rather than overwriting the archive.

39.3.4.3 Using the Document Migration Utility to Import the Archive into the Target Space

Run the Document Migration Utility specifying generated archive in the previous step to import the content into the target Content Server. For information about using the Document Migration Utility, see [Section 39.1.7.5.2, "Migrating Content Using the Document Migration Utility."](#)

Log into the Spaces application and navigate to the spaces to which content was imported and ensure the content exists.

39.3.4.4 Creating Wiki Pages in Spaces for the Content in Content Server

To use WebCenter wiki pages to display the imported wikis, perform the steps below. For more information about wiki pages, see [Section 39.3.2, "Understanding Wiki Documents and Wiki Pages."](#)

1. Log into Spaces.
2. Locate the space where the content has been uploaded.
3. Click **Actions** and select **Create and Page**.
4. Give the wiki page a **Name** and select the **Wiki** page layout.

Note that the name of the wiki page must match the name of the folder in the space folder in Spaces, which contains the wiki page of the same name.

For example, if in the space folder you have a `MarketingWiki` folder and a `MarketingWiki.htm` document, the name of the wiki page must be `MarketingWiki`.

39.4 Backing Up and Recovering WebCenter Portal 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 Portal applications on a frequent basis. The frequency of backup depends on how often the underlying information stored by WebCenter Portal 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 Portal 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*.

39.5 Troubleshooting Import and Export Issues for Spaces

This section contains the following subsections:

- [Section 39.5.1, "ResourceLimitException Issue"](#)
- [Section 39.5.2, "Spaces and Space Templates Not Available After Import"](#)
- [Section 39.5.3, "Exporting and Importing Spaces in Multibyte Languages"](#)
- [Section 39.5.4, "Page or Space Not Found Messages After Import"](#)
- [Section 39.5.5, "Space Import Archive Exceeds Maximum Upload File Size"](#)
- [Section 39.5.6, "Lists Not Imported Properly"](#)
- [Section 39.5.7, "Importing Spaces Customizations"](#)
- [Section 39.5.8, "Exporting and Importing Spaces with Services Configured"](#)

39.5.1 ResourceLimitException Issue

Problem

The `ResourceLimitException` error displays when you try to export all spaces or an entire Spaces application:

```
Weblogic.common.resourcepool.ResourceLimitException
```

Solution

Increase the maximum capacity in the JDBC connection pool. To reconfigure the connection pool, log in to the WLS Administration Console. From **Services**, select **Data Sources**, **JDBC**, and then the **Connection Pool** tab.

39.5.2 Spaces and Space Templates Not Available After Import

Problem

When you first log in to the Spaces application after the import operation, the spaces and space templates that you migrated are not available as expected. This can sometimes occur if the space/space template cache fails to refresh properly.

Solution

Refresh the space /space template cache manually using the `refreshGroupSpaceCache` and `refreshSpaceTemplateCache` WLST commands.

To completely clear the cache (all spaces):

```
refreshGroupSpaceCache(appName='webcenter', spaceNames='', syncMode=1,
updateType='all', cleanCache=1)
```

To completely clear the cache (all space templates):

```
refreshSpaceTemplateCache(appName='webcenter', spaceTemplateNames='',
syncMode=1, updateType='all', cleanCache=1)
```

For detailed command syntax and examples, see "refreshGroupSpaceCache" and "refreshSpaceTemplateCache" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

For information on how to run WLST commands, see [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

39.5.3 Exporting and Importing Spaces in Multibyte Languages

Problem

On Linux, individual space export or import fails for one or more spaces created in multibyte languages due to naming restrictions. Space names are restricted to alphanumeric and space characters ("a" through "z", "A" through "Z", "0" through "9", and the single-byte space character, which Spaces replaces with "_" (underscore)). If any other characters are used in the space name, export or import fails.

Solution

Enforce the naming restriction on the server on which Oracle WebCenter Portal is deployed. To do this, set the environment variable `LC_ALL` set to `utf-8`.

39.5.4 Page or Space Not Found Messages After Import

Problem

When you first log in to Spaces after an import operation you may see a "Page not found" or "Space not found" message if the page or space you last visited no longer exists. Such messages display because "last accessed" page information is retained during an import operation.

Solution

No action required. You will not see the message the next time you log in.

39.5.5 Space Import Archive Exceeds Maximum Upload File Size

Problem

There is a file size limitation uploading content to Spaces. If your export archive exceeds the maximum upload size then the import operation through Spaces administration fails.

Solution

Import the space archive using WLST. For details, see [Section 39.1.9.2, "Importing Individual Spaces Using WLST."](#)

Alternatively, modify the content repository upload parameter in `web.xml`. The default maximum upload size is 2 GB. See also, "[Section A.1.2, "web.xml"](#)" in [Appendix A, "WebCenter Portal Configuration."](#)

39.5.6 Lists Not Imported Properly

Problem

Lists are not importing properly due to list definition differences in the source and target systems.

Solution

Consider exporting and importing list data. This ensures that list data is consistent with the list definitions being imported.

If you choose to import without data, the list data in the target system is changed to be consistent with the imported list definitions. If a list column data type is changed, the column values are converted from the target data type to the imported data type, if possible, otherwise the value is deleted. If a list column is removed during import, the column values are deleted.

39.5.7 Importing Spaces Customizations

When you migrate a Spaces application you can choose whether certain application customizations are imported using the option "Include Customizations". [Table 39-4](#) highlights those services and task flows that store application customizations, and

which are optional on migration. [Table 39–5](#) lists application-level and space-level settings which are optional.

Note: User customization are never migrated during export and import. For more information on application customizations and user customizations, and the difference between them, see "What You Should Know About Customizing Page Components" in the *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

Table 39–4 Spaces Services - Application Customizations

Services in Spaces	Application Customizations	Optional/ Always
Analytics Service	None	
Analytics Page and Task Flows	Report preferences in page edit mode (Chart, Data Selection, Filtering, Grouping)	Optional
Announcements Service	None	
Announcement Tab	None	
Announcement Task Flow	None	
Discussions Service		
Sidebar	None	
Discussions Tab	None	
Discussion Forum Manager Task Flow	None	
Forum Task Flow	None	
Discussion Task Flows	None	
Documents Service		
Documents Tab	None	
Document Manager Task Flow	<ul style="list-style-type: none"> ■ Document Manager display preferences, such as, Description, Size, Status, Modified by, Last Modified, Links, and so on. ■ Table column settings, such as, visible columns, column sizes, and ordering. <p>See also, "Understanding the Document Manager Task Flow" in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces</i>.</p>	Optional

Table 39-4 (Cont.) Spaces Services - Application Customizations

Services in Spaces	Application Customizations	Optional/ Always
Document List Viewer Task Flow		Optional
	<p>Table column settings, such as, visible columns, column sizes, and ordering.</p> <p>In page edit mode, default fields that display document search results can be customized and additional fields can be added.</p>	
	<p>See also, "Understanding the Document List Viewer Task Flow" in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces</i>.</p>	
Content Presenter Task Flow		Optional
	<p>In page edit mode, content and display template settings.</p> <p>See also, "Understanding the Content Presenter Task Flow" in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces</i>.</p>	
Recent Documents Task Flow	None	
Events Service		
Events Tab	None	
Events Task Flow	<p>Page edit mode:</p> <ul style="list-style-type: none"> - Task flow customizations: Display Mode, Grid Start Hour, Second Timezone. - Calendars overlay properties: Name, Order, Color and Visibility. 	Optional
Lists Service		
List Tab	None	

Table 39-4 (Cont.) Spaces Services - Application Customizations

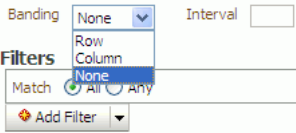
Services in Spaces	Application Customizations	Optional/ Always
List Viewer Task Flow	Page edit mode: <ul style="list-style-type: none"> <li data-bbox="821 327 1284 380">■ Banding type and interval, and column filter settings 	Optional
	 <p>The screenshot shows a configuration panel with a 'Banding' dropdown set to 'None' and an 'Interval' input field. Below it is a 'Filters' section with a 'Match' dropdown set to 'None' and radio buttons for 'All' and 'Any'. An 'Add Filter' button is at the bottom.</p>	
	<ul style="list-style-type: none"> <li data-bbox="821 569 1279 646">■ Column settings: Sort column and sort direction (ascending, descending), column sizes, and column order 	
	See also, "Working with the Lists Service" in <i>Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces</i> .	
List Manager Task Flow	None	
Mail Service		
Sidebar	None	
Mail Task Flow	None	
Notes Service		
Pages	Page edit mode: task flow and portlet customizations using 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
People Connection Service		
Activity Stream Task Flow	Display options for the Activity Stream task flow.	Optional
Portlets	Customizations/edit defaults (if any) stored in the producers.	Always
Recent Activities Service		
Resource Catalog		
RSS News Feed Service		
Search Service		
Saved Search	Shared/Private option for saved searches. Saved search customizations.	Optional
Tags Service		
Tags	None	
Tags Center	None	
Tag Sidebar	None	

Table 39–4 (Cont.) Spaces Services - Application Customizations

Services in Spaces	Application Customizations	Optional/ Always
Worklist Service	None	

Table 39–5 Spaces - Application Customizations

Spaces	Customizations	Export
Application Settings		Optional
Configuration: General tab	All properties	
Configuration: General tab	Language	
Configuration: Services tab	Default settings for Discussions, Mail, and People Connections (Profiles, Message Boards, Feedback, Connections, Activity Streams)	
Pages: Business Role Pages tab	Settings such as Set Page Defaults and display order	
Pages: System Pages	Page customizations	
Space Settings		Optional
Spaces Settings: General tab	All properties	
Spaces Settings: Pages tab	Settings such as, Set Page Defaults, Order, and Show Page Page and system page customizations	
Spaces Settings: Resource tab	Application level resources edited for use in a space	
Spaces Settings: other tabs	All properties	

39.5.8 Exporting and Importing Spaces with Services Configured

Problem

The following error message displays when you try to export a space with services configured, and try to import the same space from an instance where some or all of those services are not configured.

```
No handlers could be found for services with IDs: <list of service IDs that are not present in the target instance but present in the archive>
```

For example:

```
No handlers could be found for services with IDs: oracle.webcenter.collab.forum
oracle.webcenter.collab.rtc
```

Solution

You can work around this problem by either adding the services to the target, or removing the service-related info from the `data.xml` file of the archive as described below.

To remove service-related info:

1. Extract the archive.

The archive contains two files: `policy-store.xml` and `transport.mar`.

2. Expand the `transport.mar` into a directory.

The `data.xml` file is located in the `oracle\webcenter\lifecycle\importexport` directory.

3. Remove the service tags for all the services that are not present in the target as listed in the error message.

For the example error message above, we would need to remove the following:

```
<service id="oracle.webcenter.collab.forum" version="11.1.1.0">
  <metadataUsages>
    <metadataUsage includeBaseDocuments="YES"
includeSystemCustomizations="YES">
      <paths>
        <include
path="/oracle/webcenter/collab/forum/scopedMD/s516227ec_dde1_4991_9e18_28d487cb
3bce/**"/>
      </paths>
    </metadataUsage>
  </metadataUsages>
</service>

<service id="oracle.webcenter.collab.rtc" version="11.1.1.0"/>
```

4. Repack the `transport.mar` file by zipping the top-level directories `Oracle` and `pagedefs` into a file named `transport.mar`.
5. Repack the `export` archive by zipping the newly created `transport.mar` and the `policy-store.xml` file into an archive.
6. Import the new archive.

For the example error message above, we would need to remove the following:

Part VI

Appendixes

Part VI contains the following appendixes:

- [Appendix A, "WebCenter Portal Configuration"](#)
- [Appendix B, "Oracle HTTP Server Configuration for WebCenter Portal"](#)

WebCenter Portal Configuration

The main configuration files for WebCenter Portal applications are `adf-config.xml` and `connections.xml`. This appendix describes both these files, how to locate them, and also when to configure these files and which tools to use. Other configuration files, such as `web.xml` and `webcenter-config.xml` are described here too. See also, [Section 1.3.5, "WebCenter Portal Configuration Considerations."](#)

This appendix also outlines how to tune configuration properties for the operating system on which WebCenter Portal applications are installed, as well as WebCenter Portal applications and their back-end components.

This appendix includes the following sections:

- [Section A.1, "Configuration Files"](#)
 - [Section A.1.1, "adf-config.xml and connections.xml"](#)
 - [Section A.1.2, "web.xml"](#)
 - [Section A.1.3, "webcenter-config.xml"](#)
- [Section A.2, "Cluster Configuration"](#)
- [Section A.3, "Configuration Tools"](#)
- [Section A.4, "Tuning Oracle WebCenter Portal Performance"](#)
- [Section A.5, "Troubleshooting WebCenter Portal Application Configuration Issues"](#)
- [Section A.6, "Troubleshooting WLST Command Issues"](#)

A.1 Configuration Files

`adf-config.xml`, `connections.xml`, and `web.xml` are used to configure all WebCenter Portal applications (including Spaces) and their back-end services. In addition, the `webcenter-config.xml` configuration file, which is specific to the Spaces application, is used to configure application-wide settings.

This section describes how WebCenter Portal applications use each file and the location of these files post deployment. This section includes the following subsections:

- [adf-config.xml and connections.xml](#)
- [web.xml](#)
- [webcenter-config.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 content server that is used by the WebCenter Portal application in the development environment:

- **`adf-config.xml`** - Stores application-level settings, such as which discussions server or mail server the WebCenter Portal 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 Portal services.

See also, *Oracle Fusion Middleware Fusion Developer's Guide for Oracle Application Development Framework*.

After you deploy a WebCenter Portal application to a production environment, Oracle recommends that you use Fusion Middleware Control or WebLogic Scripting Tool (WLST) commands to reconfigure properties in these files. For example, you may want to modify connection details to point to production server instances. See also, [Appendix A.3, "Configuration Tools"](#).

The main advantage of using Fusion Middleware Control and WLST commands is that any configuration changes that you make, post deployment, are stored as *customizations* in the WebCenter Portal 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. If the application is redeployed in the future, all previous configuration changes are retained.

When a WebCenter Portal application starts up, application customizations stored in MDS are applied to the appropriate base documents and the WebCenter Portal 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*.

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 Portal 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 a Spaces application, which always has the application name `webcenter` and is deployed to the `WC_Spaces` managed server, the file name and location is always

/META-INF/mdssys/cust/adfshare/adfshare/connections.xml.xml, you might specify:

```
exportMetadata(application='webcenter', server='WC_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='WC_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 Portal application's configuration appears corrupt.

For example, consider a WebCenter Portal application built using JDeveloper called `MyPortalApp`, with a connection, created at design-time, called `myconnection`. The application was deployed to a managed server, and a URL in `myconnection` was modified. This modification is stored in MDS as a customization instruction to update `myconnection` to use the new URL. If in the future, `myconnection` is removed at design time and the application redeployed using the same MDS details, a configuration conflict occurs, that is, the customization instruction in MDS attempts to find `myconnection` but no such configuration exists.

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:

- Remove the MDS customization causing conflict manually:

1. Extract MDS customization information for `adf-config.xml` or `connections.xml`.

```
exportMetadata(application='webcenter',
server='WC_Spaces', toLocation='/tmp/mydata',
docs='/META-INF/mdssys/cust/adfshare/adfshare/adf-config.xml.xml')
```

```
exportMetadata(application='webcenter',
server='WC_Spaces', toLocation='/tmp/mydata',
docs='/META-INF/mdssys/cust/adfshare/adfshare/connections.xml.xml')
```

2. Remove the customization instruction that is causing conflict from the document.
3. Import the modified document back in to MDS.

For example:

```
importMetadata(application='webcenter',
server='WC_Spaces', fromLocation='/tmp/mydata',
docs='/META-INF/mdssys/cust/adfshare/adfshare/connections.
xml.xml')

importMetadata(application='webcenter',
server='WC_Spaces', fromLocation='/tmp/mydata',
docs='/META-INF/mdssys/cust/adfshare/adfshare/adf-config.x
ml.xml')
```

4. Restart the managed server.

- 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 application customizations for `adf-config.xml` or `connections.xml`, and all user customizations. 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

This section describes how to remove *all* post-deployment configuration for `connections.xml` or `adf-config.xml`. This operation cannot be reversed; customizations are *permanently* removed.

If you **do** want to delete MDS customizations, Oracle recommends that you use the "exportMetadata" command to save a copy of the existing files before completing the steps below.

1. Use the `exportMetadata` command to backup `connections.xml` and `adf-config.xml`.

For example:

```
exportMetadata(application='webcenter', server='WC_Spaces',
toLocation='/tmp/mydata',
docs='/META-INF/mdssys/cust/adfshare/adfshare/connections.xml
.xml')

exportMetadata(application='webcenter', server='WC_Spaces',
toLocation='/tmp/mydata',
docs='/META-INF/mdssys/cust/adfshare/adfshare/adf-config.xml.
xml')
```

2. Delete customizations for `connections.xml`, using WLST. For example:

```
deleteMetadata(application='webcenter', server='WC_Spaces',
docs='/META-INF/mdssys/cust/adfshare/adfshare/connections.xml.xml')
```

3. Delete customizations for `adf-config.xml`, using WLST. For example:

```
deleteMetadata(application='webcenter', server='WC_Spaces',
```

```
docs='/META-INF/mdssys/cust/adfshare/adfshare/adf-config.xml.xml')
```

4. Restart the WebCenter Portal application.
5. 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.

Most `web.xml` properties are fairly static so they are specified for the application at design time. If you need to modify some properties in a deployed environment, you can edit most properties through the "Configure Web Modules" screen on the "Deployment Settings" page. See also, [Figure 7-12 in Section 7.1.6.4, "Deploying Applications Using Fusion Middleware Control"](#).

There are very few 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 11.12, "Changing the Maximum File Upload Size"](#).
Note: In the Spaces application, you use the `uploadedFileMaxDiskSpace` parameter in `webcenter-config.xml` to configure a maximum upload size for files. For details, see [Appendix A.1.3, "webcenter-config.xml"](#).
- **Time after which HTTP sessions expire.** For details, see [Appendix A.4, "Tuning Oracle WebCenter Portal Performance"](#).
- **JSP page timeout value.** For details, see [Appendix A.4, "Tuning Oracle WebCenter Portal Performance"](#).

Unlike `connections.xml` and `adf-config.xml`, `web.xml` does *not* store post deployment customizations in MDS. Also, you cannot use Fusion Middleware Control or WLST to modify `web.xml` in an existing WebCenter Portal application deployment.

If you must modify settings in `web.xml` follow the appropriate instructions for your application:

- [Editing web.xml Properties for Spaces](#)
- [Editing web.xml Properties for WebCenter Portal Applications](#)

A.1.2.1 Editing web.xml Properties for Spaces

If specific `web.xml` properties need to be updated, open the Spaces EAR file, edit `web.xml`, and repackage the EAR as follows:

1. Navigate to your WebCenter Portal Oracle home directory.
2. Open the Spaces EAR file:

```
mkdir -p /tmp/my_ear
cd /tmp/my_ear
jar -xvf $WEBCENTER_HOME/archives/applications/webcenter.ear

mkdir war
cd war
jar -xvf ../spaces.war
```

3. Edit `WEB-INF/web.xml` and save the changes.
4. Create a modified `.EAR` file with the required `web.xml` properties.

```
cd /tmp/my_ear/war
jar -cvf ../spaces.war *
cd ..
rm -rf war

jar -cvf ../webcenter.ear *
```

5. Copy `/tmp/webcenter.ear` to `$WEBCENTER_HOME/archives/applications/webcenter.ear`.
6. Restart the `WC_Spaces` managed server.

At startup, this automatically deploys the newer application with the modified `web.xml`.

Caution: Future Spaces patches will overwrite this configuration change, so you must remember to repeat such configuration changes after patching, that is, you must obtain the latest `webcenter.ear` file and repeat these steps.

A.1.2.2 Editing `web.xml` Properties for WebCenter Portal Applications

Typically, when specific `web.xml` properties need to be modified, developers edit `web.xml` at design time, and regenerate the application's EAR file to include the new values.

If this is not a viable option, you can open the current application EAR file, edit `web.xml`, and repackage/redeploy the EAR as described above for the Spaces application, see [Section A.1.2.1, "Editing web.xml Properties for Spaces"](#).

A.1.3 `webcenter-config.xml`

`webcenter-config.xml` is a Spaces configuration file containing application-level settings, such as the application name and logo. Most of the properties in this file are managed through Spaces administration screens so there is no need to edit `webcenter-config.xml` directly. For more information, see "Accessing Spaces Administration Pages" and "Configuring Global Defaults" in *Oracle Fusion Middleware User's Guide for Oracle WebCenter Portal: Spaces*.

There are very few instances where you might be required to manually modify settings in `webcenter-config.xml`, for example, if you want to change the following:

- **Maximum file upload size** (`uploadedFileMaxDiskSpace`) - the default setting is 2MB.
- **Session timeout** (`wcSessionTimeoutPeriod`) - you can override the default HTTP session timeout that is set in `web.xml` (45 minutes). See also, [Section 9.9, "Setting a Session Timeout for the Spaces Application"](#).

If you want to modify these settings, you must export the latest version of `webcenter-config.xml` from MDS and modify values for `uploadedFileMaxDiskSpace` and `wcSessionTimeoutPeriod` as follows:

1. Export the latest `webcenter-config.xml` from MDS.

For example:

```
exportMetadata(application='webcenter', server='WC_Spaces',
toLocation='/tmp/mydata',
docs='/oracle/webcenter/webcenterapp/metadata/mdssys/cust/site/webcenter/webcenter-config.xml.xml')
```

Note: webcenter-config.xml is created in MDS the first time you configure "General" settings through Spaces Administration. If the file does not yet exist in MDS you can edit webcenter-config.xml directly. The file is located at:
/oracle/webcenter/webcenterapp/metadata/webcenter-config.xml

2. Open webcenter-config.xml.xml exported from MDS in a text editor and add the following snippet, as required.

To change the maximum file upload size:

```
<mds:replace
node="webcenter(xmlns(webcenter=http://xmlns.oracle.com/webcenter/webcenterapp)
)/webcenter:uploadedFileMaxDiskSpace"/>
<mds:insert
after="webcenter(xmlns(webcenter=http://xmlns.oracle.com/webcenter/webcenterapp)
)/webcenter:custom-attributes" parent="webcenter">
<uploadedFileMaxDiskSpace
xmlns="http://xmlns.oracle.com/webcenter/webcenterapp">214748364800</uploadedFileMaxDiskSpace>
</mds:insert>
```

To change the session timeout:

```
<mds:replace
node="wcSessionTimeoutPeriod(xmlns(mds_ns1=http://xmlns.oracle.com/webcenter/webcenterapp)
)/mds_ns1:value"/>
<mds:insert
after="wcSessionTimeoutPeriod(xmlns(mds_ns1=http://xmlns.oracle.com/webcenter/webcenterapp)
)/mds_ns1:type" parent="wcSessionTimeoutPeriod">
<value xmlns="http://xmlns.oracle.com/webcenter/webcenterapp">15</value>
</mds:insert>
```

3. Save and close webcenter-config.xml.xml.
4. Import the updated webcenter-config.xml.xml file to MDS.

For example:

```
importMetadata(application='webcenter', server='WC_Spaces',
fromLocation='/tmp/mydata',
docs='/oracle/webcenter/webcenterapp/metadata/mdssys/cust/site/webcenter/webcenter-config.xml.xml')
```

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, since the MDS repository is shared across all nodes, all WebCenter Portal configuration changes done on one node 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 Portal Application Deployments"](#).

In WebCenter Portal 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 WebCenter Portal's services (Analytics, Activity Graph, Announcements, Discussions, Documents, Events, Mail, Instant Messaging and Presence, Search, Worklists) you must restart the application's managed server.

There are two 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 Portal application and any changes that you make to existing connections take effect immediately too.

If you edit configuration files 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 Spaces and other WebCenter Portal application deployments. This section outline which tools are available.

Note: Most WebCenter Portal configuration parameters are immutable and cannot be changed at run time unless otherwise specified.

Post deployment, always use Fusion Middleware Control or WebLogic Scripting Tool (WLST) commands to review the latest configuration or make configuration changes. In Fusion Middleware Control you will mostly use WebCenter Portal 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 use the same MDS details when you redeploy the application, all configuration performed using these tools is preserved.

What Configuration Tool to Use

You can use any tool for post-deployment configuration. However, if you intend to repeat the configuration steps multiple times, for example, when provisioning newer instances or for automation, screen-based configuration using tools such as Fusion Middleware Control becomes less efficient. In such cases, Oracle highly recommends that you write WLST scripts to perform the required configuration.

All WebCenter Portal configuration operations possible through Fusion Middleware Control are available using WebCenter Portal's WLST commands. You can also use WLST scripts to configure other components, for example, to deploy applications, create managed servers, set MDS properties for an application, configure data sources,

and so on. If you want help to automate domain configuration, you can record configuration actions in the WLS Administration Console as a series of WLST commands and then use WLST to replay the commands. For more details on this topic, see "Recording WLST scripts" in *Oracle Fusion Middleware Introduction to Oracle WebLogic Server*.

Tip: Where Oracle documentation describes steps in the WLS Administration Console, consider automating the process using the "Record" option.

Another way to configure deployment specific properties is through the WebCenter Portal application's deployment plan. Typical properties changed on deployment include:

- Host/port properties for connections
- Standard J2EE artifacts in `web.xml`

See also, [Section 7.1.6, "Deploying the Application to a WebLogic Managed Server"](#).

Note: While reconfiguration is possible this way, any metadata repository and ADF connection configuration changes that you make are not saved as part of the deployment plan, that is, they are saved in the archive that is deployed. Therefore, your configuration changes must be repeated on subsequent redeployments.

If you redeploy your application multiple times, Oracle recommends that you use Fusion Middleware Control or WLST commands to perform your post-deployment configuration. This way, configurations changes are saved in MDS and remain intact on redeployment.

A.4 Tuning Oracle WebCenter Portal Performance

Refer to the chapter "Oracle WebCenter Portal Performance Tuning" in the *Oracle Fusion Middleware Performance and Tuning Guide* for information on tuning the parameters listed in [Table A-1](#):

Table A-1 WebCenter Portal Performance Tuning

Performance Tuning	Parameters	File
Environment	System Limit	
	JDBC Data Source (settings for MDSDS and WebCenterDS)	
	JRockit virtual machine (JVM) arguments	<code>setDomainEnv.sh</code>
WebCenter Portal Applications	HTTP Session Timeout	<code>web.xml</code>
	JSP Page Timeout	<code>web.xml</code>
	ADF Client State Token	<code>web.xml</code>
	MDS Cache Size and Purge Rate	<code>adf-config.xml</code>
	Concurrency Management	<code>adf-config.xml</code>
	CRUD APIs (Create, Read, Update and Delete)	<code>adf-config.xml</code>

Table A-1 (Cont.) WebCenter Portal Performance Tuning

Performance Tuning	Parameters	File
Spaces Applications	Spaces Session Timeout	webcenter-config.xml
Back-end Components ¹		
Announcements Service	Connection Timeout	connections.xml
Discussions Service	Connection Timeout	connections.xml
Instant Messaging and Presence (IMP) Service	Connection Timeout	connections.xml
Mail Service	Connection Timeout	connections.xml
RSS News Feed Service	Refresh Interval	adf-config.xml
Search Service	Number of Saved Searches Displayed, Number of Results Displayed, various Timeouts	adf-config.xml
WSRP Producers	Connection Timeout	connections.xml
Oracle PDK-Java Producers	Connection Timeout	connections.xml
OmniPortlet	Connection Timeout	connections.xml
Portlet Service	Locale Support, Portlet Timeout, Portlet Cache Size	adf-config.xml

¹ Performance of back-end servers, for example, Worklists, Oracle WebCenter Content Server, and so on, should be tuned as described in guidelines for those back-ends.

A.5 Troubleshooting WebCenter Portal Application Configuration Issues

This section includes the following sub sections:

- [Section A.5.1, "WebCenter Portal Does Not Display in the Application Deployment Menu in Fusion Middleware Control"](#)
- [Section A.5.2, "Configuration Options Unavailable"](#)
- [Section A.5.3, "Configuration Performed in One Application Reflects in Another"](#)
- [Section A.5.4, "Spaces Application Logs Indicate Too Many Open Files"](#)

A.5.1 WebCenter Portal Does Not Display in the Application Deployment Menu in Fusion Middleware Control

Problem

After logging into Fusion Middleware Control, you cannot find the **WebCenter Portal** option in the **Application Deployment** menu.

Solution

Ensure the following:

- Deployed application is an ADF application.
The **WebCenter Portal** option does not display for applications that are not developed using ADF.
- Deployed application is up and running.

- Deployed application contains accurate information about the MDS repository and partition, and the MDS repository is accessible to the application. To verify this information, 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>
```

- 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>

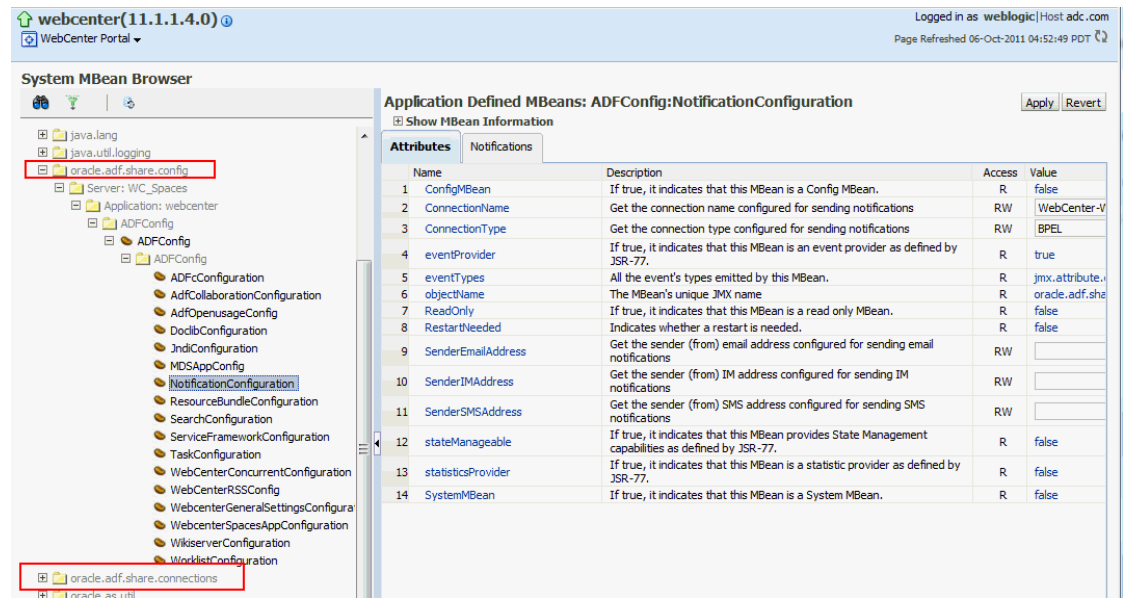
  <listener-class>oracle.adf.mbean.share.config.ADFConfigLifecycleCall</l
istener-class>
</listener>
<listener>
  <description>ADF Connection MBeans</description>
  <display-name>ADF Connection MBeans</display-name>

  <listener-class>oracle.adf.mbean.share.connection.ADFConnectionLifeCycleCal
lBack</listener-class>
</listener>
```

- MBeans are registered for the WebCenter Portal 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 A-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 A-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.

A.5.2 Configuration Options Unavailable

Problem

When you try to configure a WebCenter Portal application through 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 A.5.1, "WebCenter Portal Does Not Display in the Application Deployment Menu in Fusion Middleware Control."](#)

A.5.3 Configuration Performed in One Application Reflects in Another

Problem

You configured a WebCenter Portal 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 Portal application to use a different MDS repository or partition, see section "Managing the Oracle Metadata Repository" in *Oracle Fusion Middleware Administrator's Guide*.

A.5.4 Spaces Application Logs Indicate Too Many Open Files

Problem

Spaces is inaccessible or displaying error messages and the diagnostic log files indicates that there is an issue with 'too many open files'.

Solution

Do the following:

- Check the number of file handles configured on each of the back-end servers, primarily the database, and increase appropriately.
- If the problem persists after increasing the file handles, check the value of `fs.file-max` in the `/etc/sysctl.conf` file and increase the value appropriately.

A.6 Troubleshooting WLST Command Issues

This section includes the following sub sections:

- [Section A.6.1, "None of the WebCenter Portal WLST Commands Work"](#)
- [Section A.6.2, "WLST Commands Do Not Work for a Particular Service"](#)
- [Section A.6.3, "A Connection with the Name Connection_Name Already Exists"](#)
- [Section A.6.4, "WLST Shell is Not Connected to the Oracle WebLogic Managed Server Instance"](#)
- [Section A.6.5, "Application with the Same Name Already Exists in a Domain"](#)
- [Section A.6.6, "Application with the Same Name Already Exists on a Managed Server"](#)
- [Section A.6.7, "Already in Domain Runtime Tree Message Displays"](#)

See also, [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands"](#).

A.6.1 None of the WebCenter Portal WLST Commands Work

Problem

You are unable to run any WLST commands.

Solution

Ensure the following:

- Always run WebCenter Portal WLST commands from your **WebCenter Portal Oracle home directory** (`WC_ORACLE_HOME/common/bin`).

If you attempt to run WebCenter Portal WLST commands from the wrong directory you will see a `NameError`.

- No files other than Python are stored in the WLST source directory: `WC_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 `WC_ORACLE_HOME/common/bin/wlst/lib`.

A.6.2 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 Portal 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 A.6.1, "None of the WebCenter Portal WLST Commands Work."](#)

If generic commands work, then run test commands to check WebCenter Portal-specific commands for syntax errors. Run the appropriate WLST check command (see [Table A-2](#)).

See also, [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

Table A-2 File Names and WLST Commands for WebCenter Portal Service

Service Name	File Name	WLST Command
Activity Graph	ActivityGraph.py	metadataAdminCheck()
Activity Stream	ActivityStream.py	asCheck()
Analytics	Analytics.py	analyticsCheck()
	OpenUsage.py	openusageCheck()
Discussions and Announcements	Forum.py JiveAdmin.py	fcpcCheck()
Documents	Doclib.py	doclibCheck()
External Applications	ExtApp.py	extCheck()
Space Events	CommunityWLST.py	ceCheck()
Instant Messaging and Presence	Imp.py	rtcCheck()
Mail	Mail.py	mailCheck()
Notifications	Notification.py	notificationCheck()
Personal Events	Personal.py	peCheck()
Producers		
PDK-Java Producers	Pdk.py	pdkCheck()
WSRP Producers	Wsrp.py	wsrpCheck()
Pagelet Producers	Ensemble.py	ensembleCheck()
Producer Helper	Producer.py	producerHelperCheck()
RSS News Feed	RSS.py	rssCheck()
Search	Ses.py	sesCheck()
Worklist	Bpel.py	bpelCheck()

Table A–2 (Cont.) File Names and WLST Commands for WebCenter Portal Service

Service Name	File Name	WLST Command
Export/Import - WebCenter Portal applications	Lifecycle.py	lifecycleCheck()
Export/Import - Spaces and Template	ExtImp.py	expimpCheck()
WebCenter Portal - General		
Service Framework	WcServiceFwk.py	serviceFwkCheck()
General Settings	WebCenterGeneralSettings.py	generalSettingsCheck()
Spaces and SOA	WebCenterSpacesSOA.py	spaceCheck()

A.6.3 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 Portal applications. This error occurs when you try to create a connection with a name that is in use. Ensure that you use a unique name for your connection.

A.6.4 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 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

A.6.5 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 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

A.6.6 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 "registerWSRPProducer" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

See also, [Section 1.13.3.1, "Running Oracle WebLogic Scripting Tool \(WLST\) Commands."](#)

A.6.7 Already in Domain Runtime Tree Message Displays

Problem

While running a WLST command, the following message displays:

```
Already in Domain Runtime Tree
```

Solution

None required. This is for information only.

Oracle HTTP Server Configuration for WebCenter Portal

For Oracle WebCenter Portal components that run on Oracle WebLogic Server, you can set Oracle HTTP Server (OHS) as the frontend to Oracle WebLogic Server. Some scenarios that require OHS as the frontend are:

- For OSSO to function properly between Site Studio and Oracle Content Server. This is achieved through `mod_osso` of OHS.
- The adequate distribution of load across the Oracle WebLogic Server cluster nodes. This is achieved through `mod_wl` of OHS.
- OHS is also required for OAM's WebGate component.
- OHS is used as a reverse proxy.

In these cases, you must configure the `mod_wl_ohs` module to allow requests to be proxied from an OHS to Oracle WebLogic Server. For information, see the section "Configure the `mod_wl_ohs` Module on Oracle HTTP Server" in *Oracle Fusion Middleware Administrator's Guide for Oracle HTTP Server*.

Sample `mod_wl_ohs.conf`

After you have configured the `mod_wl_ohs` module using the Fusion Middleware Control, the `mod_wl_ohs.conf` file looks similar to [Example B-1](#). The default location of this file is:

```
OHS_HOME/Oracle_WT1/instances/instance1/config/OHS/ohs1/mod_wl_ohs.conf.
```

Example B-1 Spaces - Sample `mod_wl_ohs.conf` File

```
# Spaces Application
<Location /webcenter>
  SetHandler weblogic-handler
  WeblogicHost webcenter.example.com
  WeblogicPort 8888
</Location>
<Location /webcenterhelp>
  SetHandler weblogic-handler
  WeblogicHost webcenter.example.com
  WeblogicPort 8888
</Location>
<Location /rss>
  SetHandler weblogic-handler
  WeblogicHost webcenter.example.com
  WeblogicPort 8888
</Location>
```

```

    <Location /rest>
      SetHandler weblogic-handler
      WeblogicHost webcenter.example.com
      WeblogicPort 8888
    </Location>
# Discussions
    <Location /owc_discussions>
      SetHandler weblogic-handler
      WeblogicHost discuss.example.com
      WeblogicPort 8890
    </Location>
# SES Search
    <Location /rsscrawl>
      SetHandler weblogic-handler
      WeblogicHost ses.examplet.com
      WeblogicPort 7777
    </Location>
    <Location /sesUserAuth>
      SetHandler weblogic-handler
      WeblogicHost ses.example.com
      WeblogicPort 7777
    </Location>
# Portlets
    <Location /portalTools>
      SetHandler weblogic-handler
      WeblogicHost webcenter.example.com
      WeblogicPort 8889
    </Location>
    <Location /wsrp-tools>
      SetHandler weblogic-handler
      WeblogicHost webcenter.example.com
      WeblogicPort 8889
    </Location>
    <Location /pagelets>
      SetHandler weblogic-handler
      WeblogicHost webcenter.example.com
      WeblogicPort 8889
    </Location>
# Personalization
    <Location /wcps>
      SetHandler weblogic-handler
      WeblogicHost webcenter.example.com
      WeblogicPort 8891
    </Location>
# Activity Graph
    <Location /activitygraph-engines>
      SetHandler weblogic-handler
      WeblogicHost webcenter.example.com
      WeblogicPort 8891
    </Location>
# UCM
# Web server context root for Oracle WebCenter Content Server
    <Location /cs>
      SetHandler weblogic-handler
      WeblogicHost ucm.example.com
      WeblogicPort 16200
    </Location>
# Enables Oracle WebCenter Content Server authentication
    <Location /adfAuthentication>
      SetHandler weblogic-handler

```

```

        WeblogicHost ucm.example.com # Same as /cs entry
        WeblogicPort 16200          # Same as /css entry
    </Location>
# SAML SSO
    <Location /samlacs/acs>>
        SetHandler weblogic-handler
        WeblogicHost ucm.example.com
        WeblogicPort 16200
    </Location>
# BPEL Server
    <Location /workflow>
        SetHandler weblogic-handler
        WeblogicHost soa.example.com
        WeblogicPort 8001
    </Location>
# Virtual Hosts - Sharepoint
    <VirtualHost *:7777>
        ServerName webtier-spaces.example.com
        <Location />
            SetHandler weblogic-handler
            WeblogicHost webcenter.example.com
            WeblogicPort 8888
        </Location>
        <Location /webcenter>
            Deny from all
        </Location>
        <Location /webcenterhelp>
            Deny from all
        </Location>
        <Location /rest>
            Deny from all
        </Location>
    </VirtualHost>

```

SSL Directives

If you have configured SSL, then the following additional directives are required:

- `WLProxySSL ON`
- `WLProxySSLPassthrough ON`

For example, `mod_wl_ohs.conf` entries looks like [Example B-2](#):

Example B-2 Spaces - `mod_wl_ohs.conf` File with SSL Directives

```

# Spaces Application
    <Location /webcenter>
        SetHandler weblogic-handler
        WeblogicHost webcenter.example.com
        WeblogicPort 8888
        WLProxySSL ON
        WLProxySSLPassthrough ON
    </Location>
    <Location /webcenterhelp>
        SetHandler weblogic-handler
        WeblogicHost webcenter.example.com
        WeblogicPort 8888
        WLProxySSL ON
        WLProxySSLPassthrough ON
    </Location>

```

...

Frontend Listening Host and Frontend Listening Port

If the Oracle HTTP Server (OHS) frontend is also the site entry point, use the Oracle WebLogic Server Administration Console to set the `FrontEnd Host` and `FrontEnd HTTP Port` *for each* server that uses the OHS frontend.

Glossary

About mode

A **portlet mode** that typically displays information such as copyright, version, and author of the portlet.

Activity Stream

In the **People Connections service**, a feature for viewing the application activities tracked for you and other users.

Activity Graph

A WebCenter Portal service that provides suggestions of people, items, and spaces that users may be interested in interacting with.

The engine used by the Activity Graph service to provide a central repository for actions that are collected by enterprise applications. The data stored in the activity graph is analyzed to calculate ranks for nodes, predict new actions, and make recommendations.

Activity Rank

Determines the relevance of a search result.

administrator

In the Spaces application 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.
- Spaces administrator: A user responsible for customizing 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 enables requests to be made to the server without fully re-rendering the page. Ajax enables rich client-like applications to use standard internet technologies.

Analytics service

A WebCenter Portal service offers real-time usage and activity reporting for your portal. In the Spaces application, users can track and analyze Spaces traffic and usage.

Announcements service

A WebCenter Portal 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 customization

Performed by an administrator, all users see the change. These are static changes to an application that affect a site or sites that do not involve changes to the application's code or schema.

See also [user customization](#) and [personalization](#)

Application Development Framework

See [Oracle ADF](#).

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 application background color, screen fonts, and, with some skins, the shapes and images used for application buttons and icons. In the Spaces application, the administrator chooses the default application skin and Spaces users may change the application skin on the General tab of the Preferences dialog.

application templates

WebCenter Portal provides templates for creating two kinds of applications: Framework applications and Portlet Producer applications. Templates ensure that the right technology scopes are set, tag libraries added, and required Java classes are added to the class path. Once you do this, relevant components are included to the Component Palette and relevant context menus become available in JDeveloper.

See also [Framework application template](#) and [Portlet Producer Application template](#).

authenticated user

A user who is logged into a WebCenter Portal application. Credentials of this user are verified against the identity store. By default, an authenticated user can access public information. To access secured information, such as pages and [portlets](#), this user must be authorized through the policy and credential store.

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 Framework application only (all ADF resources in the application remain accessible), or authentication *and*

authorization to enforce credentials for users to access the Framework 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](#).

AviTrust Portal Demonstration for WebCenter Portal

An enterprise banking application built using Oracle Fusion Middleware, including Oracle WebCenter Portal: Framework and WebCenter Portal: Spaces, used to provide examples of WebCenter Portal functionality.

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

A layout component available through Oracle WebCenter Portal's Composer. A container that enables the placement of content on a page created in the Spaces application. In Composer, a Box is rendered as a rectangle comprised of dashed lines. In a Framework application, 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 administrators in the Spaces application, 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 Home space 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](#).

calendar overlay

The ability to display multiple calendars in a single Events task flow.

Change Mode Button component

In the Composer tag library that enables users to change from page View mode to page Edit mode.

Change Mode Link component

A component provided in the Composer tag library that enables users to change from page View mode to page Edit mode.

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.

Child Components

The components contained within a parent component. For example, the task flows contained within a Box layout component are the child components of the Box.

See also [Box layout component](#) and [parent component](#).

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.

CMIS

Content Management Interoperability Services (CMIS) standard defines a domain model and Web services and Restful AtomPub bindings that can be used by applications to work with one or more Content Management repositories or systems.

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 Composer, that provides access to all the content you can add to a WebCenter Portal application page.

component developer

The developer who builds components (such as portlets, [JavaServer Faces](#) components, and web services).

Component Properties

A dialog, accessed from Composer, that provides access to a component's parameters, display options, child components, style settings, and associated events.

Connections

In the [People Connections service](#), a feature for establishing a social network with other application users.

Composer

A seamlessly integrated environment for populating, revising, and configuring portal 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.

container

An application program or subsystem in which the program building block, known as a **component**, is run.

container runtime option

A JSR 286 feature that provides a way to customize the behavior of the portlet container and therefore customize the runtime environment.

content integration services

Services provided by **Oracle WebCenter Portal** to enable developers to display content from a **content repository**, such as by creating **data controls**.

Content Presenter

A feature of the **Documents service** that enables end users to select and search content items and then display those items using available display templates. Oracle WebCenter Portal provides out-of-the-box templates for displaying single and multiple content items on your pages. You can also define custom templates for the content that you want to display in your **Framework application**, or for selection by end users at runtime.

content repository

A specialized storage and management mechanism that provides such features as author-based versioning, full text searching, and content categorization and attribution. A content repository 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 **Framework application**, you can create content repository data controls for the following content repositories: **Oracle Portal**, **Oracle WebCenter Content**, third-party repositories that support the Java Content Repository (JCR) standard, and your local file system.

credential provisioning page

A **JSF** (* .jspx) page used for authenticating to an **external application**. At runtime, 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

Provides storage for login credentials for its associated domain. It also preserves the login credentials that a user provides for authentication to an **external application**. Credential store is usually combined with the policy store as a single logical store.

Although the credentials stored in the credential store are used during subsequent logins for authentication, the main function of this store is to provide authorization for those accounts.

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 rendered on the header or the Actions menu of a Show Detail Frame component surrounding a task flow. Custom actions can represent actions that were defined in the task flow when it was created. For example, at design time a developer can build a task flow with custom personalization settings. At runtime, users can access these settings through icons or Actions menu items provided in the task flow's surrounding chrome (or Show Detail Frame).

custom attribute

In the Spaces application, custom attributes specify 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 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 space template.

custom page

Any page created by a user rather than one provided out of the box.

custom display template

A Content Presenter display template is a JSFF file (JSF page fragment) that defines how Content Presenter renders content items on a Framework application page. WebCenter Portal provides several out-of-the-box display templates to get you started, or, you can create your own templates.

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 space moderator to meet a specific Home space or 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 Portal 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](#).

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.

default language (application-level)

A display language specified by the Spaces administrator that is used when users log in to the Spaces application. The Spaces administrator sets the application-level default

language on the **General** tab of the **Administration** page. Individual users can set their own user-level default language on the General tab of the Preferences dialog.

default language (user preference)

A user-specified display language that is rendered when the user logs in to the Spaces application. This language selection lasts until the user specifies a different default language. It can be overridden by a session language, but returns as the default when the session cookie is purged or expires. This value is set on the **General** tab of the Preferences dialog.

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](#).

delegated administration

Provides a mechanism for securing portal resources based on user roles. You apply delegated administration to a page hierarchy, and the specific security assignments are automatically propagated down through the hierarchy through pages and sub pages.

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 Portal services](#) provides a special deployment profile, the [Framework 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 (Spaces)

A view, in [Composer](#), that provides a WYSIWYG representation of a page and its components.

See also [Source view \(Spaces\)](#).

discoverable space

A space that can be found by anyone logged into the Spaces application, for example through a search. Any **Public** or **Private** space is discoverable. Discoverable spaces are listed on the **Spaces** page when **All Spaces** is selected from the **Show** list. Users

wishing to join the space can request membership through self-service (if enabled) or by contacting the space moderator.

Discussions service

A WebCenter Portal service that provides a means of creating and participating in discussion forums.

display language

Controls the language in which application user interface elements, such as buttons, field labels, and screen text, are rendered in the browser. The order of precedence for Framework application display language settings from weakest to strongest is: browser setting, application setting, user preference setting, session setting, space setting.

Documents page

A predefined page provided in every Spaces group and Home space that includes the Document Manager task flow for managing content.

Documents service

A WebCenter Portal service that provides several task flows that offer a variety of formats to display folders and files on a page. You can choose the task flows appropriate for your application to provide features for accessing, adding, and managing folders and files; configuring and viewing file and folder properties; and searching file and folder content in the connected content repositories.

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. **Framework applications** are deployed using both a generic EAR file, which contains the application and the respective runtime customization, and a targeted EAR file, which contains 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 [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 286 portlets only.) A **portlet mode** that enables personalization of a JSR 286 portlet. Edit Defaults mode is a display mode for the JSR 286 portlet's properties. In a **Framework 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 shorthand 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 **Framework application**, EL expressions are encapsulated in the characters "{" and "}" and typically come in the form `#{object.data}` where *object* represents any Java object or **Oracle 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 Portal service that provides calendars for scheduling meetings, appointments, and so on. In the Spaces application, it provides calendars to record events relevant to the specific space. You can also integrate the Events service with Microsoft Exchange Server to enable individual users to access their personal calendars in their Home space. Personal calendars are also available in Framework application.

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**.

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 pages in the Spaces application and external web sites.

Federated Portal Adapter

See [FPA](#).

Feedback

In the [People Connections service](#), a feature for posting informal appraisals for and receiving informal appraisals from other application users.

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 Framework applications.

Framework application

A Framework application is built on top of the ADF using the [WebCenter Portal's Extension for Oracle JDeveloper](#). This application combines web content, portlets, content integration, and collaborative services for the end user. Developers and administrators can create a Framework application based on their roles and skill levels in the organization.

A portal also includes page hierarchies, navigation models, and delegated administration.

Framework application administrator

The administrator responsible for maintaining the [Framework application](#). For example, in Spaces, the administrator performs tasks such as implementing the branding for the Framework application, making new content available, modifying pages, and granting and revoking privileges.

Contrast with systems administrator who has administrative rights for entire Fusion Middleware functions. The Fusion Middleware administrator is also responsible for deploying, setting up, and configuring the Framework application, and performing on-going administrative tasks for the Framework application and other WebCenter Portal components through Fusion Middleware Control.

Framework application developer

The developer who plans, builds, and maintains a [Framework application](#) using the Oracle Application Development Framework, [Oracle JDeveloper](#), and [Oracle WebCenter Portal](#).

Framework application end user

The runtime user of the [Framework application](#), who accesses pages, portlets, and content, and personalizes portlets (assuming the appropriate privileges).

Framework application life cycle

The process of creating and testing a Framework 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 life cycle of an application also includes performing further enhancements, restaging, and then redeploying the application to the production system.

Framework application template

A JDeveloper template which includes WebCenter Portal: Framework features like site navigation, page hierarchies, delegated administration, and page templates.

See also [application templates](#) and [Portlet Producer Application template](#).

Full Screen Mode (Spaces)

A view mode that opens the 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 Portal. From Fusion Middleware Control, you can monitor and administer a [farm](#) (such as Oracle WebCenter Portal).

Fusion Order Demo (FOD)

See [AviTrust Portal Demonstration for WebCenter Portal](#).

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](#).

Home space

A work area within 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.

HTML Markup layout component

A layout component available through Composer. A simple HTML component that renders raw HTML and JavaScript mark-up inline on the page.

Hyperlink layout component

A layout component available through Composer. A link to an internal or external web page. For designers of Framework applications, this is the runtime equivalent of a Go Link component.

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.

Identity Propagation

For a Framework application and associated content repositories, selecting this option allows propagation of current user's identity across the application and processes. The propagated identity is verified on the receiver's side, and then it is used to make decisions such as assigning role based access control.

Image layout component

A layout component available through Composer. An illustration that can include a hyper link. For designers of Framework 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 286 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 Portal](#), initialization parameters are entered into the `portlet.xml` file.

Instant Messaging and Presence service

A WebCenter Portal service that enables users to observe the presence status of other authenticated users and provides instant access to interaction options, such as instant messages and emails.

Integrated Development Environment

See [IDE](#).

Integrated WLS

Integrated WebLogic Server. A WLS instance used as a platform for pretesting Framework application deployments on a local computer. Integrated WLS also contains preconfigured portlet producers and several useful prebuilt portlets.

Iterative development

Iterative development lets you make changes to your Framework application while it is running on the Integrated WebLogic Server and immediately see the effect of those changes simply by refreshing the current page in your browser. The iterative development feature works by disabling certain optimization features. Iterative development allows developers to work more quickly and efficiently when building a Framework application.

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.

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 286](#).

Java Specification Request

See [JSR 286](#).

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 **APIs** 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 286

Java Specification Request (JSR) 286. 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=286>.

JSR 170

See **JCR 1.0**

JSR 329

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 page created in the Spaces application.

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 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.

life cycle

See [Framework application life cycle](#).

Lightweight Directory Access Protocol (LDAP)

See [LDAP](#).

Links service

A WebCenter Portal service that provides a means of creating a bidirectional association between two objects, thus setting up easy access between those objects.

Lists service

A WebCenter Portal service that provides a means of creating lists and exposing them for placement on application pages at runtime. At design time, you can make the Lists task flow available in your runtime Resource Catalog. At runtime, users can add the task flow from the Catalog to a page and use the task flow to create lists.

Lists page

A predefined page that displays the space's current lists.

Look and feel

A look and feel file determines the appearance of your application, from the placement and behavior of elements on a portal page to the colors used in the portlet title bars. The look and feel is determined by skins, navigations, page templates, layouts, content display templates, and other similar components.

Mail service

A WebCenter Portal service for exposing familiar email functionality in 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.

See also [enterprise mashup](#).

MBean Browser

In Fusion Middleware Control, MBean browsers enable the administrator to perform specific monitoring and configuration tasks and browse MBeans for an Oracle WebLogic Server or a selected application.

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.

MDS repository

An application server and Oracle relational database that keep metadata in these areas: a file-based repository, dictionary tables accessed by build-in functions, and a metadata registry. One of the primary uses of MDS is to store customizations and persisted personalization for Oracle applications.

Message Board

In the [People Connections service](#), a feature for posting messages to and receiving messages from other application users.

metadata

Information about a content item, such as title, author, or security group. Metadata is used to describe, find, and group content items. Also referred to as content information.

Model-View-Controller

See [MVC](#).

moderator

A Spaces user who is responsible for managing a particular space. A space moderator can add and remove members, invite new members, enable self registration, provide and update space metadata, and manage the services available to the space.

Movable Box layout component

A layout component available through Composer. A container that enables the placement of content on a page created in the Spaces application. Movable Boxes, along with their content, can be moved around on the page. For designers of Framework applications, this is the runtime 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 Spaces page

A predefined page that displays a list of all the spaces available to the currently logged in user. The user can select from the **Show** menu to display **All Spaces**, only spaces of which the user is a member (**Joined by Me**), or only spaces of which the user is the moderator (**Moderated by Me**).

navigation

WebCenter Portal provides three navigation components to create portal navigation. These components are: Breadcrumb navigation, menu navigation, and tree navigation.

navigation model

Navigation models provide data to the navigation user interface and enable navigation to resources in your application, such as pages, page hierarchies, task flows, external sites, portlets, and other entities. You can configure navigation models at both design time and runtime.

Notes service

A WebCenter Portal service that provides useful features for writing personal notes and reminders. This service is available only in Spaces, and not in Framework applications.

Notifications service

A WebCenter Portal service that provides an automated means of triggering notices across different messaging channels, such as phone, mail, Worklist, and so on. Messages are triggered when the spaces and application objects to which you have subscribed change.

Oracle ADF

Oracle 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.

OAM

See [Oracle Access Manager \(OAM\)](#).

OHS

See [Oracle HTTP Server \(OHS\)](#).

OmniPortlet

A component of [Oracle WebCenter Portal](#) 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 Spaces and Framework applications. OAM is the recommended single sign-on solution for Oracle WebCenter Portal 11g installations.

Oracle ADF Faces

Oracle [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 WebCenter Content: Content Server

A content repository 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 WebCenter: Content Server is a component of Oracle WebCenter Content.

Oracle WebCenter Portal's Discussions Server

Backend discussions server for the Discussions and Announcements services.

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 Framework 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 a repository for provisioning users and groups. By default, the [Oracle Single Sign-On \(OSSO\)](#) 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 329, the Oracle JSF Portlet Bridge enables application developers to expose a JSF application or task flow as a JSR 286 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.

See also [Oracle WebLogic Portal](#).

Oracle Secure Enterprise Search (SES)

Provides easy-to-use search for public and secure data, with unified ranking results. With Framework applications, Oracle SES is set as the default and preferred search platform.

With Spaces applications, WebCenter Portal's internal live search adapters are set as the default search platform; however, large-scale implementations should be configured to use Oracle SES for best performance.

Oracle Single Sign-On (OSSO)

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 WebCenter Content's Site Studio

A powerful, flexible web development application suite that offers a comprehensive approach to designing, building, and maintaining enterprise-scale web sites. Site Studio uses Oracle WebCenter Content: Content Server as the main repository for a web site.

In WebCenter, Content Presenter integrates with Site Studio to allow you to create, access, edit, and display Site Studio contributor data files in either a Site Studio region template or a custom Content Presenter display template.

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 WebCenter Content

Provides a flexible, secure, centralized, web-based repository that manages all phases of the content life cycle: from creation and approval to publishing, searching, expiration, and archival or disposition. It enables contributors to easily contribute content from native desktop applications, efficiently manage business content through rich library services, and securely access that content anywhere using a web browser. All content, regardless of content type, is stored in the web repository or database for management, reuse and access.

Oracle WebCenter Portal

A suite of services that enables you to build Oracle WebCenter Portal applications. Oracle WebCenter Portal 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 Portal includes:

- [Oracle WebCenter Portal services](#)
- [Oracle WebCenter Portal: Framework](#)
- [content integration services](#)

- [Oracle ADF](#)
- [Oracle Secure Enterprise Search \(SES\)](#)
- [Oracle WebCenter Portal's Discussions Server](#)
- Mobile Services
- Portlet Pack

Oracle WebCenter Portal: Framework

A set of features provided by [Oracle WebCenter Portal](#) that augments the Java Server Faces (JSF) environment by providing additional integration and runtime customization options. It integrates capabilities historically included in portal products, such as site navigation, page hierarchies, portlets, customization, personalization, and integration, directly into the fabric of the JSF environment. This eliminates artificial barriers for the user and provides the foundation for developing context-rich applications. You can selectively add only desired Oracle WebCenter Portal components or services to your framework application.

Oracle WebCenter Portal's Pagelet Producer

Provides a collection of useful tools and features that facilitate dynamic pagelet development.

Oracle WebCenter Portal services

A collection of Web 2.0 services that expose social networking and personal productivity features through various services.

- [Activity Graph](#)
- [Announcements service](#)
- [Analytics service](#)
- [Discussions service](#)
- [Documents service](#)
- [Events service](#)
- [Instant Messaging and Presence service](#)
- [Links service](#)
- [Lists service](#)
- [Mail service](#)
- [Notes service](#)
- [Notifications service](#)
- [People Connections service](#)
- [Personalization for WebCenter Portal](#)
- [Polls service](#)
- [Recent Activities service](#)
- [RSS service](#)
- [Search service](#)
- [Tags service](#)
- [Worklist service](#)

Oracle WebCenter Portal: Spaces

A WebCenter Portal application built using JSE, Oracle ADF, WebCenter Portal: Framework, WebCenter Portal: Services, and Composer. In the production documentation, it is commonly referred as **Spaces application (Spaces)**.

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

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/technetwork>.

Oracle WebLogic Portal

WebLogic Portal enables you to provide a user interface to integrate your applications. WebLogic Portal lets you surface application data and functionality from heterogeneous environments into an integrated, dynamic, and customizable web-based portal user interface that can simultaneously support multiple devices. In addition to a powerful portal framework and its J2EE security foundation, WebLogic Portal provides many business services, such as content management, communities, personalization, search, and user management. WebLogic Portal provides a virtual content repository that lets you federate external content management systems into a single management interface. You can then build portals using content in those external resource. WebLogic Portal also provides a WLP content repository for creating and managing content.

Page Customizable component

A component provided in the 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 hierarchy

A model that associates pages in a parent-child relationship, where any page can have one or more sub pages. This parent-child model not only helps define the overall structure of the portal, but also allows child pages to inherit the security policies from their parent.

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. It also 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 Properties

A dialog, accessed from Composer, that provides access to a page's display options, security settings, and parameters.

page scheme

Determines the background image used in the page. The Spaces application provides several default page schemes and an option for specifying a custom page scheme.

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 template

Lets you specify view elements that you intend to be common to all of your pages. A page template file is a JSPX file that includes ADF layout components and other elements. Typically, page templates define a page layout, with headers, footers, and content areas. In addition, the page template usually specifies the positioning and style of the navigation UI for your pages.

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 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.

parent component

A component that contains other components, such as a Box layout component that contains task flows. The Box is the parent component of the task flows. In contrast, the task flows are the Box's child components.

See also [Child Components](#).

participant

A Spaces user who can manipulate the content of a space. A participant can upload and share documents, initiate and take part in chats with other members, create discussion topics, 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 Portal](#). 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.

People Connections service

A WebCenter Portal service that provides social networking tools for creating, interacting with, and tracking the activities of one's enterprise connections.

See also, [Activity Stream](#), [Connections](#), [Feedback](#), [Message Board](#), and [Profile](#).

personalization

Dynamic changes to an application's behavior based on user context, facilitated by Personalization for WebCenter Portal.

See also [application customization](#) and [user customization](#)

Personalization for WebCenter Portal

A WebCenter Portal service that enables you to deliver content within your application to targeted application users based on selected criteria. Personalization for WebCenter Portal also provides a declarative means for specifying dynamic application flow.

personal page

A page created by a user in his or her Home 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.

See also, [Profile](#).

Polls service

A WebCenter Portal service that enables you to create, edit, and take online polls on your application pages. Polls let you survey your audience (such as their opinions and their experience level) and check whether they can recall important information, and gather feedback on the efficacy of presentations.

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 application template

See [application templates](#).

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 and programmatic portlets built through WebCenter's JSR 286, PDK-Java Portlet wizards, and other portlet building tools.

portlet event

A JSR 286 feature that allows portlets to react to actions or state changes not directly related to an interaction of the user with the portlet.

portlet filter

A JSR 286 feature that allows on-the-fly transformations of information in both the request to and the responses from a portlet. A portlet filter is a reusable piece of code that can transform the content of portlet requests and portlet responses.

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 [Framework application template](#) and [producer](#).

predefined page

A page created by the Spaces application to perform a specific function. Examples of predefined pages include, Welcome pages, Search pages, and Documents pages.

Predeployment Tool

A utility for [Framework applications](#) that assists you in configuring 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, for example, to export and import 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 communication link between portlet consumers (such as a [Framework 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 Portal](#) 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 286](#), .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.

Profile

In the [People Connections service](#), a feature for viewing and managing information about yourself, such as your contact information, manager, and direct reports, and for viewing this information about other application users.

programmatically portlets

Portlets constructed in a non-declarative manner using [APIs](#). Also referred to as *hand-* or *manually-coded* portlets.

public render parameters

A JSR 286 feature that enables portlets to share parameter values, allowing a form of interportlet communication.

public space

A space that is available to all users, even those who are not logged in to the Spaces application.

public page

A page within the Spaces application that is available to all users, even those who are not logged in to the application.

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 Portal 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 Portal service that provides a means of tracking recent activities in a Framework application.

recipe

A weighted list of similarity calculations. The weighting of each calculation determines its significance in deciding the overall recommendation score. Recommendations are ordered by their total recommendation score.

resize handle

A user interface element in a task flow chrome increasing or decreasing the height of the task flow.

resource

Items users can manage through the Resource Manager, like page templates, skins, task flows, navigations, and so on. Spaces categorizes resources under the following categories: Structure, Look and Layout, and Mashups.

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.

Resource Index

The starting point for accessing WebCenter Portal REST APIs. Sending a GET request to the Resource Index URI returns a list of links to entry points for all available services.

Resource Manager

Enables users with the appropriate privileges to continue developing the portal after the application has been deployed. Using the Resource Manager users can also download runtime portal resources (from Framework applications and Spaces) and import them into Oracle JDeveloper for further development. These resources can then be exported from JDeveloper and uploaded back into the deployed application.

resource type

Defines the type of resource that a WebCenter Portal REST API link identifies. Use resource types to determine the response bodies for GET requests and allowable request bodies for POST and PUT. Also use `resourceType` attributes on entities to uniquely identify their type.

REST APIs

Oracle WebCenter Portal provides a set of web-based REST (REpresentational State Transfer) APIs for retrieving and modifying server data dynamically from the client. REST APIs are available for [Discussions service](#), [People Connections service](#), and [Spaces application \(Spaces\)](#).

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.

Round-trip development

Round-trip development refers to features and techniques that allow you to retrieve resources from a deployed, runtime portal back to JDeveloper for maintenance or enhancement. After modifying a resource in JDeveloper, you can use the Resource Manager to upload the resource back to the deployed portal. WebCenter Portal's round-trip development features provide a simple, convenient way to modify portal resources without redeploying the entire application.

RSS reader

An RSS reader provided with the Spaces application that incorporates public news feeds from external sources onto application pages. This RSS reader is available only in Spaces, and not in Framework applications.

RSS service

A WebCenter Portal 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 service

A WebCenter Portal service that enables the discovery of information and people in an application, returning only the results users are authorized to see

Secure Enterprise Search

See [Oracle Secure Enterprise Search \(SES\)](#).

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 the Spaces application, thus creating themselves an identity store 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 space. Moderators can customize certain aspects of this page.

service ID

In Expression Language, the string that identifies a particular service. For example, the string `oracle.webcenter.collab.announcement` is the service ID for the Announcements service.

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 (from log on to log off). If the user clears browser cookies, the display language reverts to the user-level default language, if specified, then to the application-level default language set by the Spaces administrator. 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 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](#).

similarity calculation

Used by the Activity Graph service to provide a similarity score (a number between zero and one) that designates how similar two objects are to each other given a specific criterion. The weighting of each calculation determines its significance in deciding the overall recommendation score. Recommendations are ordered by their total recommendation score.

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 (Spaces)

A view, in Oracle WebCenter Portal's Composer, that provides a selectable structural representation of a page and its components.

See also [Design view \(Spaces\)](#).

space

A work area within Spaces that supports a group of people of any size that is organized around an area of interest or a common goal.

Spaces application (Spaces)

A web-based application that offers the very latest technology for social networking, communication, collaboration, and personal productivity. 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.

space icon

An image displayed alongside space names on the Spaces page in My Spaces to help other users with identification and location.

space logo

An image displayed on the Home space page to provide a visual identity for the space. The Home space logos also display alongside the space name at the top of the page in Full Screen Mode.

space member

A user who is participating in a space. Members can be added or invited to a space, or they can subscribe to a space themselves if self-registration is enabled.

space owner

A user who initially created a space. The space owner is automatically also a moderator of the space.

space template

A starting point for creating a new space. Spaces includes several out-of-the-box templates to get you started, and you can create custom space templates using existing spaces as the basis.

space Unavailable page

A predefined page that displays when a space member tries to open a space that is temporarily offline. Moderators can customize this page.

Spaces application administrator

See [administrator](#).

Spaces Switcher

A menu showing three areas: **Recent Spaces** lists up to ten recently accessed spaces, followed by spaces to which current user most recently gained access. **My Spaces** lists all spaces to which the current user has access, in alphabetical order. A list of links provides direct access from the menu to the Home space, the Spaces browser page, and the Create a Space dialog.

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 Portal 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 [space template](#), [application templates](#), and [custom display template](#).

Text layout component

A layout component available through Composer. A rich text editor for providing static page text. For designers of Framework applications, this is the runtime equivalent of a Rich Text Editor component.

Unauthorized Access page

A predefined page that is shown when someone without access permission tries to open a page.

URL parameter

See [private parameter](#).

user customization

Changes that affects only a user's own work space.

See also [application customization](#) and [personalization](#)

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](#).

Virtual Content Repository

Virtual Content Repository (VCR) enables you to plug in multiple, heterogeneous content repositories.

viewer

Spaces users who can look at the information in a space but cannot contribute any of their own.

View mode

([JSR 286](#) portlets only.) A [portlet mode](#) that enables you to display a JSR 286 portlet on a page that can contain other portlets. It is the only required mode for JSR 286 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](#).

Web 2.0

Technologies, such as wiki, RSS, and blogs, that enable the construction of highly interactive web applications.

See also [Oracle WebCenter Portal services](#).

Web Application Archive file

See [WAR](#).

Web Clipping portlet

A browser-based declarative tool that enables you to integrate any web application with your [Framework 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 onto a *.jspx page.

Web Page layout component

A layout component available through Composer. A means of embedding another web site, wiki, or blog within the context of a page which is created in the Spaces application. For designers of Framework 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 Portal Application

A WebCenter Portal application based on [Oracle WebCenter Portal: Framework](#) or [Oracle WebCenter Portal: Spaces](#).

WebCenter Portal's 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 [Framework applications](#) in [Oracle JDeveloper](#).

WebCenter Portal: Framework

See [Oracle WebCenter Portal: Framework](#).

WebCenter Portal systems administrator

See [administrator](#).

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 the Spaces application.
- Personal Welcome page: A predefined page that introduces users to their Home 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 wiki content.

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 Portal.

Worklist service

A WebCenter Portal 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 286](#), .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.

XSL

Extensible Stylesheet Language (XSL) is the language used within style sheets to transform or render XML documents.

A

- access protocols, 1-8
- Activity Graph engines
 - about, 12-1
 - Collaborative Filtering Engine, 12-8
 - Gathering Engine, 12-8
 - Rank Engine, 12-8
 - running
 - on a schedule, 12-9
 - on demand, 12-9
- Activity Graph provider, 20-4
 - configuring, 20-12
- Activity Graph service
 - about, 12-1
 - Activity Graph engines, 12-1, 12-8
 - Activity Rank, 12-13
 - configuring, 12-7
 - customizing reason strings, 12-10
 - deleting metadata, 12-12
 - exporting metadata, 12-11
 - exporting provider configuration, 12-12
 - importing metadata, 12-12
 - Oracle SES, 12-13
 - preparing data, 12-8
 - prerequisites, 12-7, 13-5
 - QRPPs, 12-3
 - recipe, 12-3
 - registering an Analytics Collector, 13-9
 - schema customizations, 12-11
 - similarity calculation, 12-3
- Activity Rank, 12-13
- Activity Stream
 - archiving, 18-2
- addWorklistConnection (WLST command), 23-12
- ADF (Application Development Framework), 1-3
- ADF Client State Token, A-9
- ADF libraries, 1-7, 1-8
- ADF security
 - about, 28-3
 - permission-based authorization, 28-6
 - role-mapping based authorization, 28-6
- adf-config.xml, 1-9, A-9
- Admin role (WebLogic Server), 1-13
- administration server
 - See WebLogic Server Administration Console
- administration tools
 - See Fusion Middleware Control
 - See Spaces Administration pages
 - See System MBean Browser
 - See WebLogic Scripting Tool (WLST)
 - See WebLogic Server Administration Console
- administrator role
 - granting for Oracle WebCenter
 - Discussions, 14-15
 - granting to a user (Framework application), 36-14
 - granting to nondefault user, 14-15
 - revoking from default user, 14-16
- Analytics Collector
 - about, 13-2
 - configuring, 13-6
 - registering with a Framework application, 13-9
- Analytics service
 - about, 13-2
 - managing connections, 13-1
 - partitioning data, 13-14
 - prerequisites, 13-5
 - purging data, 13-14
 - registering an Analytics Collector, 13-9
 - task flows, 13-3
 - troubleshooting, 13-14
- Announcements service
 - configuring for WebCenter Services
 - Portlets, 24-20
 - connection
 - activating, 14-10
 - creating, 14-5
 - deleting, 14-12
 - managing, 14-1
 - modifying, 14-11
 - performance issues and actions, 38-40
 - performance metrics, 38-9
 - performance tuning, A-10
 - troubleshooting, 14-17
- anonymous-role (Framework application), 36-17
- application roles (Framework application)
 - assigning to enterprise groups, 36-11
 - assigning to users, 36-11
 - changing role assignments, 36-13
 - creating, 36-15
 - custom roles, 36-7
 - deleting, 36-18

- granting permissions, 36-16
- permissions, 36-7
- revoking from a user, 36-14
- authenticated-role (Framework application), 36-18
- authentication methods (external applications), 26-6
- authentication, of REST services, 27-4
- automatic login (external applications), 26-5

B

- backup and recovery
 - about, 39-72
 - WebCenter back-end components, 39-72
- basic authentication
 - external applications, 25-15
 - pagelet producer resources, 25-15
- BASIC authentication method, 26-6
- Blog Metrics (analytics task flow), 13-3
- BPPEL servers
 - configuring notifications, 19-8
 - configuring Spaces workflows, 9-2
 - hosting Spaces workflows, 9-2
 - LDAP identity store, 23-7
 - managing connections, 23-5
 - performance issues and actions, 38-40
 - performance metrics, 38-10
 - prerequisites, 23-6
 - single sign-on, 23-7
 - Worklist service requirements, 23-6
 - WS-Security, 23-7

C

- CFE (Collaborative Filtering Engine), 12-8
- Change Center, 1-17
- checklists
 - administering the Spaces application, 3-1
 - administering WebCenter Portal applications, 5-1
 - getting Framework applications up and running, 4-1
 - getting Spaces application up and running, 2-1
- CKEditor
 - WebCenter Services Portlets, 24-21
- CLIENT_STATE_MAX_TOKENS setting, A-9
- cluster
 - Analytics Collector configuration, 13-6
 - cluster configuration, A-7
 - discussion server configuration, 14-3
 - WebCenter Portal application deployment, 1-10
- CMIS provider, 20-4, 20-11
- Collaborative Filtering Engine, 12-8
- command-line configuration (WLST), 1-18
- Composer, 1-3
- composite applications, 1-5
- compression, and REST APIs, 27-4
- concurrency management, A-9
- configuration files
 - adf-config.xml, 1-9, A-1
 - connections.xml, 1-9, A-1
 - handling conflicts, A-3

- webcenter-config.xml, A-1, A-6
- web.xml, A-1
- connections
 - configuring MDS repository, 10-1, 10-4
 - managing post deployment
 - Framework applications, 6-6
 - Spaces application, 6-3
 - setting up Analytics, 13-1
 - setting up content repositories, 11-1
 - setting up Discussions and Announcements, 14-1
 - setting up Events, 15-1
 - setting up Instant Messaging and Presence, 16-1
 - setting up Mail, 17-1
 - setting up pagelet producers, 25-1
 - setting up portlet producers, 24-1
 - setting up Search, 22-1
 - setting up Worklists, 23-5
- connections.xml, 1-9, A-10
- Content Presenter
 - configuring for Personalization, 20-17
- content repositories
 - about connections, 11-1
 - active connection, 11-48
 - changing active connection
 - using Fusion Middleware Control, 11-49
 - using WLST, 11-49
 - connection information files, 11-3
 - default connection, 11-48
 - deleting connections
 - using Fusion Middleware Control, 11-55
 - using WLST, 11-55
 - file system, 11-38
 - managing, 11-1
 - managing connection properties (WebCenter Spaces)
 - using Fusion Middleware Control, 11-56
 - using WLST, 11-56
 - modifying connections
 - using Fusion Middleware Control, 11-50
 - using WLST, 11-50
 - Oracle Content Server, 11-3
 - Oracle Portal, 11-37
 - performance metrics, 38-11
 - registering
 - using Fusion Middleware Control, 11-40
 - using WLST, 11-48
- Content Server
 - exporting application content, 39-15
 - exporting space documents, 39-29
 - importing application content, 39-16
 - importing space documents, 39-29
- createBPPELConnection (WLST command), 23-11
- createDiscussionForumConnection (WLST command), 14-9
- createExtAppConnection (WLST command), 26-8
- createIMPConnection (WLST command), 16-21
- createJCRContentServerConnection (WLST command), 11-48
- createJCRFileSystemConnection (WLST command), 11-48

- createJCRPortalConnection (WLST command), 11-48
- createJCRSharePointConnection (WLST command), 11-36
- createMailConnection (WLST command), 17-12
- createPersonalEventConnection (WLST command), 15-10
- createSESConnection (WLST command), 22-12
- credential mapping (Pagelet Producers), 25-15
- credential provisioning (external applications)
 - about, 26-1
 - public credentials, 26-7
 - shared credentials, 26-7
- CRUD APIs, A-9
- custom managed servers, 1-7
- customizations
 - migrating, 7-24
 - storing in MDS, A-2

D

- data source
 - choosing, 7-13
 - global, 7-13
 - local, 7-13
- database connection
 - about, 10-1
 - creating, 10-1
- database connection, changing (WebCenter repository), 10-5
- deleteAGAction (WLST command), 12-12
- deleteAGNodeClass (WLST command), 12-12
- deleteAGProviderAssignment (WLST command), 12-12
- deleteAGQRPPRegistration (WLST command), 12-12
- deleteAGRANKCalculation (WLST command), 12-12
- deleteAGSimilarityCalculation (WLST command), 12-12
- deleteAllAGMetadata (WLST command), 12-12
- deleteConnection (WLST command), 11-55, 14-13, 15-13, 16-24, 17-17, 22-16, 23-14, 26-10
- deleteDocumentsSpacesProperties (WLST command), 11-56
- deployment
 - about, 7-3
 - checking application connections, 7-36
 - checking data source connections, 7-36
 - choosing the data source, 7-13
 - EAR file, 7-4
 - global data source, 7-13
 - local data source, 7-13
 - migrating customizations, 7-24
 - post-deployment configuration, 7-35
 - post-deployment security configurations, 7-35
 - Spaces, 1-15
 - undeploying WebCenter Portal applications, 7-25
 - using Fusion Middleware Control, 7-14
 - using JDeveloper, 7-14
 - using WLS Administration Console, 7-21
 - using WLST, 7-19

- WebCenter Portal applications, 7-1, 7-12
- WebLogic Managed Server, creating, 7-4
- WebLogic Managed Server, provisioning, 7-4
- deregisterOOTBProducers (WLST command), 24-15
- deregisterPDKJavaProducer (WLST command), 24-15
- deregisterSampleProducers (WLST command), 24-15
- deregisterWSRPPProducer (WLST command), 24-15
- desktop integration
 - virtual host, 31-79
- diagnostic log files, 1-11
- Discussion Metrics (analytics task flow), 13-4
- discussions server
 - configuration files
 - exporting data, 39-13
 - exporting discussions for a space, 39-25
 - granting administrator role to nondefault user, 14-15
 - importing data, 39-13
 - importing discussions for a space, 39-27
 - managing connections, 14-1
 - performance metrics, 38-9, 38-16
 - prerequisites, 14-2
 - registering, 14-5
 - revoking administrator role, 14-16
 - WS-Security, 14-4
- Discussions service
 - configuring for WebCenter Services Portlets, 24-20
 - connection
 - activating, 14-10
 - creating, 14-5
 - deleting, 14-12
 - managing, 14-1
 - modifying, 14-11
 - performance issues and actions, 38-40
 - performance metrics, 38-16
 - performance tuning, A-10
 - permissions (Framework application), 36-7
 - troubleshooting, 14-17
 - usage reports (analytics), 13-4
- distribution lists (WebCenter Spaces), 17-19
- Document Metrics (analytics task flow), 13-3
- Documents service
 - configuring for WebCenter Services Portlets, 24-19
 - content repositories, 11-2
 - exporting space content, 39-29
 - importing space documents, 39-29
 - performance issues and actions, 38-40
 - performance metrics, 38-11
 - usage report (analytics), 13-3
- dynamic group, 29-47

E

- EAR files, 7-4
- enterprise groups, assigning to roles, 36-11
- Enterprise Manager

- See Fusion Middleware Control
- events server
 - managing connections, 15-1
 - prerequisites, 15-5
 - registering, 15-8
 - SSL, 15-6
- Events service
 - connection
 - activating, 15-10
 - creating, 15-8
 - deleting, 15-12
 - managing, 15-1
 - modifying, 15-11
 - testing, 15-13
 - performance issues and actions, 38-41
 - performance metrics, 38-18
 - prerequisites, 15-5
 - troubleshooting, 15-14
 - using Microsoft Exchange Server 2003, 15-7
 - using Microsoft Exchange Server 2007, 15-5
- export and import
 - about, 39-1
 - exporting a space, 39-36
 - exporting a space template, 39-38
 - exporting resources
 - Framework applications, 39-44
 - WebCenter Portal: Spaces, 39-39
 - Framework applications
 - about, 39-41
 - exporting portlet client metadata, 39-43
 - exporting WebCenter Portal services metadata and data, 39-45
 - importing portlet client metadata, 39-43
 - importing WebCenter Portal services metadata and data, 39-47
 - migrating application security policies, 39-48
 - prerequisites, 39-42
 - importing a space, 39-37
 - importing a space template, 39-38, 39-39
 - importing resources
 - Framework applications, 39-44
 - WebCenter Portal: Spaces, 39-40
 - migration tools, 39-42
 - Spaces
 - customizations and personalizations, 39-74
 - exporting discussions, 39-25
 - exporting documents, 39-29
 - exporting using WLST, 39-73
 - importing discussions, 39-27
 - importing documents, 39-29
 - migrating back-end components, 39-24
 - troubleshooting, 39-72
 - Spaces application
 - about, 39-1, 39-2
 - customizations, 39-4
 - prerequisites, 39-4
 - WebCenter Portal applications
 - exporting data, 39-48
 - importing data, 39-49
 - migrating data, 39-48
- WebCenter Portal: Spaces
 - back-end components, 39-4
 - credential store, 39-6, 39-10
 - exporting Content Server data, 39-15
 - exporting discussions, 39-13
 - exporting entire producer metadata, 39-18
 - exporting LDAP identity store, 39-5
 - exporting Oracle WebLogic Communications Server, 39-17
 - exporting using Fusion Middleware Control, 39-19
 - exporting using WLST, 39-22
 - importing Content Server, 39-16
 - importing discussions, 39-13
 - importing entire producer metadata, 39-18
 - importing LDAP identity store, 39-6
 - importing Oracle WebLogic Communications Server, 39-17
 - importing using Fusion Middleware Control, 39-23
 - importing using WLST, 39-24
 - policy store, 39-8, 39-12
- exportAGMetadata (WLST command), 12-11
- exportAGProviderConfiguration (WLST command), 12-12
- exportGroupSpaces (WLST command), 39-36
- exportGroupSpaceTemplates (WLST command), 39-38
- exportMetadata (WLST command), 39-45, A-2
- exportPortletClientMetadata (WLST command), 24-14, 39-43
- exportWebCenterApplication (WLST command), 39-22
- exportWebCenterResource (WLST command), 39-40
- external applications
 - about, 26-1
 - adding extra login fields, 26-7
 - deleting
 - using Fusion Middleware Control, 26-10
 - using WLST, 26-10
 - managing post deployment
 - Framework applications, 6-6
 - Spaces application, 6-3
 - modifying
 - using Fusion Middleware Control, 26-8
 - using WLST, 26-9
 - performance issues and actions, 38-41
 - performance metrics, 38-20
 - registering
 - using Fusion Middleware Control, 26-4
 - using WLST, 26-8

F

- file system
 - connection parameters, 11-47
 - limitations in WebCenter, 11-38
 - security considerations, 11-38
- file-based identity store
 - exporting and importing credential store, 39-10

- exporting and importing policy store, 39-12
- files, maximum upload size, 11-59, A-6
- Framework applications
 - configuring OAM, 32-4
 - configuring SAML SSO, 32-7
 - export and import, 39-41
 - getting applications up and running (checklist), 4-1
 - home page in Fusion Middleware Control, 6-5
 - monitoring performance, 38-52
 - permissions, 36-7
 - single-sign on, 32-1
 - starting and restarting
 - using Fusion Middleware Control, 8-6
 - using WLST, 8-6
 - stopping
 - using Fusion Middleware Control, 8-6
 - using WLST, 8-7
 - viewing and configuring logs, 38-54
- Fusion Middleware administrators, 3-1
 - Admin role (WebLogic Server), 1-13
 - Monitor role (WebLogic Server), 1-13
 - Operator role (WebLogic Server), 1-13
 - roles and responsibilities (Framework applications), 4-1
 - roles and responsibilities (Oracle WebCenter Portal: Spaces), 2-1
 - roles and responsibilities (WebCenter Portal applications), 5-1
- Fusion Middleware Control
 - about, 1-16
 - changing content repository active connection, 11-49
 - deploying Portlet Producer applications, 24-18
 - deploying WebCenter Portal applications, 7-14
 - exporting Spaces application, 39-19
 - importing WebCenter Portal Spaces, 39-23
 - managing
 - Analytics service connections, 13-1
 - Announcements service connections, 14-1
 - content repository connections, 11-1
 - Discussions service connections, 14-1
 - Events service connections, 15-1
 - Instant Messaging and Presence service connections, 16-1
 - Mail service connections, 17-1
 - portlet producer connections, 24-13
 - Search service connections, 22-1
 - Worklist service connections, 23-5
 - monitoring Framework applications, 38-1
 - navigating to
 - Framework application home page, 6-5
 - Spaces application home page, 6-2
 - operation summary, 1-14
 - redeploying WebCenter Portal applications, 7-30
 - registering
 - PDK-Java producers, 24-10
 - WSRP producers, 24-3
 - registering an MDS schema, 7-9

- starting, 6-1
- undeploying WebCenter Portal applications, 7-25

G

- garbage collector, A-9
- Gathering Engine, 12-8
- GET authentication method, 26-6
- getRssProxyConfig (WLST command), 9-6

H

- heap size, A-9
- HTTP server
 - See* Oracle HTTP Server
- HTTP Session Timeout, A-9, A-10

I

- identity store
 - aggregating multiple identity stores, 29-29
 - See* LDAP identity store
 - See* LDAP identity store
- IMAP
 - connection configuration, 17-9
 - Mail service connections, 17-2
 - SSL security configuration, 17-8
- IMP (Instant Messaging and Presence) service connection
 - activating, 16-21
 - creating, 16-21
 - deleting, 16-23
 - managing, 16-1
 - modifying, 16-22
 - performance issues and actions, 38-41
 - performance metrics, 38-22
 - performance tuning, A-10
- import and export, 39-1
 - performance issues and actions, 38-41
 - performance metrics, 38-23
- importAGMetadata (WLST command), 12-12
- importGroupSpaces (WLST command), 39-37, 39-39
- importMetadata (WLST command), 39-47
- importPortletClientMetadata (WLST command), 24-14, 39-43
- importWebCenterApplication (WLST command), 39-24
- importWebCenterResource (WLST command), 39-41, 39-45
- installation
 - Analytciis Collector, 13-5
 - BPEL server, 23-6
 - discussions server, 14-2
 - events server, 15-5
 - mail server, 17-6
 - Oracle SES, 22-7
 - presence server, 16-2
 - WebCenter Portal, 1-13
- Instant Messaging and Presence (IMP)
 - See* IMP

J

J2EE application deployment, 6-5
Java keystore
 complex topology, 34-25
 simple topology
 typical topology, 34-14
JDBC data source, A-9
JKS
 See Java keystore
JNDI Name, 10-5
JRF libraries, 1-8
JRockit, A-9
JSP Page Timeout parameter, A-9
JVM arguments, A-9
JVM_ARGS argument, 1-19

K

keystore
 See Java keystore

L

language support
 about, 37-2
 adding a new language, 37-7
LCS
 See Microsoft Live Communications Server, 16-1
LDAP identity store
 about, 28-5
 adding users, 29-10
 aggregating using libOVD, 29-29
 BPEL server requirements, 23-7
 exporting, 39-5
 exporting and importing credential store, 39-6
 exporting and importing policy store, 39-8
 external LDAP, 28-7
 moving the administrator account, 29-19
 importing, 39-6
 Microsoft Lync requirements, 16-18
 Microsoft Office Communications Server (OCS)
 requirements, 16-11
 Microsoft Office Live Communications Server
 (LCS) requirements, 16-5
 tuning, 29-8
LDIF files
 adding users to LDAP, 29-15
 creating, 29-16
 root node, 30-2
libOVD, 29-29
Links service, permissions (Framework
 applications), 36-7
listAnalyticsEventTypes (WLST command), 13-14
listDocumentsSpacesProperties (WLST
 command), 11-56
listJCRSharePointConnection (WLST
 command), 11-36
Lists service
 performance issues and actions, 38-41
 performance metrics, 38-23

 permissions (Framework applications), 36-7
 permissions for WebCenter Services
 Portlets, 24-22
Lock and Edit (WebLogic Administration
 Console), 1-17
Login Metrics (analytics task flow), 13-3
logs
 configuring, 38-54
 Framework applications, 38-54, 38-55
 log file locations, 1-11
 Spaces, 38-54
 viewing, 38-54
 WebCenter Portal
 Spaces, 38-55

M

mail servers
 configuring notifications, 19-8
 managing connections, 17-1
 performance metrics, 38-25
 prerequisites, 17-5
 registering, 17-8
Mail service
 configuring for WebCenter Services
 Portlets, 24-20
 connection
 activating, 17-13
 creating, 17-8
 deleting, 17-16
 managing, 17-1
 modifying, 17-15
 performance issues and actions, 38-42
 performance metrics, 38-25
 performance tuning, A-10
 setting up connections, 17-1
 troubleshooting, 17-18
managed servers
 about, 1-6
 creating, 7-4
 provisioning, 7-4
 SOA, 9-2
 starting and stopping, 8-2
 startup order, 1-8
 WC_Collaboration, 1-7
 WC_Portlet, 1-7
 WC_Spaces, 1-7
 WC_Uilities, 1-7
MDS (Metadata Service) repository
 creating, 7-5
 registering, 7-5
MDS Cache Size parameter, A-9
MDS Purge Rate parameter, A-9
MDS repository
 application startup failure
 base file locations, A-2
 configuration files, 1-9
 configuring, 10-1, 10-4
 customizations, 1-9, A-2
 setting MDS cache size, A-9

- setting MDS purge rate, A-9
- MDS schema
 - creating, 7-5
 - registering, 7-5
 - registering using Fusion Middleware Control, 7-9
 - registering using WLST, 7-11
- memory size, A-9
- Metadata Service (MDS) repository
 - creating, 7-5
 - registering, 7-5
- Microsoft Exchange Server
 - registering, 17-8
 - setting up events connections, 15-5
 - using Microsoft Exchange Server 2003, 15-7
 - using Microsoft Exchange Server 2007, 15-5
 - setting up mail connections, 17-1
- Microsoft Live Communications Server
 - about, 16-2
 - LDAP identity store, 16-5
 - performance metrics, 38-22
 - prerequisites, 16-2
 - registering, 16-18
 - setting up connections, 16-1
 - SSL security, 33-37
- Microsoft Lync
 - about, 16-11
 - LDAP identity store, 16-18
 - prerequisites, 16-2
 - registering, 16-18
 - setting up connections, 16-1
- Microsoft Office Communication Server
 - SSL security, 33-37
- Microsoft Office Communications Server
 - LDAP identity store, 16-11
 - performance metrics, 38-22
 - prerequisites, 16-2
 - registering, 16-18
 - setting up IMP connections, 16-2
- migrateSecurityStore (WLST command), 39-6
- migrating customizations, 7-24
- mod_osso module, B-1
- mod_wl_ohs module, B-1
- modifying provider connection settings, 20-8
- Monitor role (WebLogic Server), 1-13
- monitoring performance
 - common performance issues and actions, 38-8
 - Framework applications, 38-52
 - metric collection, 38-2
 - WebCenter Portal
 - Spaces, 38-48
 - WebCenter Portal services, 38-3

N

- Node Manager, 8-2
- Notes service
 - performance issues and actions, 38-42
 - performance metrics, 38-27
- notifications, 19-1 to 19-19
 - activities that trigger messages, 19-3

- connection types
 - about, 19-8
 - setting with Fusion Middleware Control, 19-11
 - setting with WLST commands, 19-12
- creating custom notification templates, 19-13
- overwriting default templates, 19-14, 19-17
- preferences in Spaces, 19-7
- prerequisites, 19-8
 - configuration, 19-9
 - installation, 19-9
 - limitations, 19-9
- setting up default preferences, 19-2
- subscription default settings
 - effect on connections, 19-5
 - effect on feedback, 19-6
 - effect on Message Board, 19-5
 - effect on Spaces management, 19-6
- testing connections, 19-17
- troubleshooting, 19-18

O

- OAM
 - configuring for Framework applications, 32-4
 - See* Oracle Access Manager
- OAM-SSO, 14-19
- OBJECTGUID attribute, 37-6, 37-8
- OCS (Office Communications Server)
 - See* Microsoft Office Communications Server
- OmniPortlet
 - about, 1-8, 8-2, 24-1
 - performance tuning, A-10
- open-files-limit, A-9
- Operator role (WebLogic Server), 1-13
- OPSS Trust Service, 20-5
 - configuring, 20-5, 29-49
 - configuring cross-domain trust, 20-7
- Oracle Access Manager
 - Access Server, 31-3
 - configuring, 31-2
 - configuring using scripts, 31-14
 - Identity Assertion Provider, 31-3
 - installing the 11g WebTier, 31-7
 - logout from SSO applications, 28-3
 - single sign-on, 28-8
 - topology and components, 31-2
 - WebGate, 31-3
- Oracle Application Development Framework, 1-3
- Oracle Content Server
 - configuring, 11-9
 - item level security, 11-8
 - OracleTextSearch, 11-8
 - SES Crawler, 11-7
 - configuring identity store, 29-29
 - connection parameters, 11-42
 - prerequisites, 11-3
 - security considerations, 11-3
 - verifying signatures, 33-33
- Oracle DMS, 1-8

- Oracle Enterprise Manager
 - See* Fusion Middleware Control
- Oracle HTTP Server, B-1
- Oracle Internet Directory, 28-7, 29-2, 29-17, 30-5, 33-31
- Oracle Metadata Repository
 - See* MDS repository
- Oracle Platform Security Services, 28-3, 28-6
 - APIs, 28-7
- Oracle Portal
 - configuring, 11-37
 - connection parameters, 11-47
 - installing, 11-37
 - limitations in WebCenter, 11-37
 - prerequisites, 11-37
- Oracle Secure Enterprise Search (SES), 22-1
 - configuring
 - for WebCenter Portal applications, 22-17
 - for WebCenter Spaces, 22-37
 - managing connections, 22-1
 - overview, 22-2
 - performance metrics, 38-38
 - prerequisites, 22-7
 - registering, 22-10
 - SSL security, 22-10
- Oracle SES
 - See* Oracle Secure Enterprise Search (SES)
- Oracle Single Sign-On (OSSO), 31-37
 - components, 31-38
 - configuring, 31-37
- Oracle SOA Suite, 9-2
- Oracle Web Services Manager (wsm-pm), 1-8
- Oracle WebCenter
 - default security, 28-1, 28-4
- Oracle WebCenter Portal
 - about, 1-1
 - administration tools, 1-16
 - administrative roles, 1-13
 - architecture, 1-2
 - configuration files, A-1
 - configuration overview, 1-9
 - configuration tools, A-8
 - external dependencies, 1-8
 - installing, 1-13
 - log file locations, 1-11
 - managed servers, 1-7
 - performance monitoring, 1-15
 - topology, 1-6
- Oracle WebCenter Portal: Framework, 1-3
- Oracle WebCenter Portal: Spaces
 - getting started, 2-1
- Oracle WebLogic Communications Server
 - exporting, 39-17
 - importing, 39-17
 - performance metrics, 38-22
- Oracle WebLogic Scripting Tool
 - See* WLST
- override language bundle, 37-5
- owc_discussions application, 1-8, 8-2

P

- page permissions (Framework applications), 36-7
- Page service
 - Page Traffic analytics task flow, 13-3
 - performance issues and actions, 38-42
 - performance metrics, 38-28
- Page Traffic (analytics task flow), 13-3
- Page Traffic analytics task flow, 13-3
- PDK-Java producers
 - performance tuning, A-10
 - registering
 - in Framework applications, 24-12
 - in WebCenter Portal: Spaces, 24-12
 - using Fusion Middleware Control, 24-10
 - using WLST, 24-12
 - securing, 35-6
 - testing connections, 24-13
- People Connections locator, 20-5, 20-13
- People Connections service
 - Activity Stream, 18-2
 - performance issues and actions, 38-42
 - performance metrics, 38-35
- performance issues and actions
 - Announcements service, 38-40
 - Discussions service, 38-40
 - Documents service, 38-40
 - Events service, 38-41
 - external applications, 38-41
 - IMP service, 38-41
 - import and export, 38-41
 - Lists service, 38-41
 - Mail service, 38-42
 - Notes service, 38-42
 - Page service, 38-42
 - People Connections service, 38-42
 - portlet producers, 38-42
 - RSS service, 38-43
 - Search service, 38-43
 - Worklist service, 38-40
- performance metrics
 - Announcements service, 38-9
 - Discussions service, 38-16
 - Documents service, 38-11
 - Events service, 38-18
 - external applications, 38-20
 - Import and Export service, 38-23
 - Instant Messaging and Presence service, 38-22
 - Lists service, 38-23
 - Mail service, 38-25
 - metric collection, 38-2
 - Notes service, 38-27
 - Page service, 38-28
 - People Connections service, 38-35
 - Polls service, 38-36
 - portlet producers, 38-29
 - portlets, 38-31
 - Recent Activities service, 38-38
 - RSS service, 38-37
 - Search service, 38-38
 - Spaces, 38-44

- viewing performance information, 38-48
- WebCenter Portal services, 38-3
- Worklist service, 38-10
- permissions
 - to use Framework applications, 36-7
 - to use Fusion Middleware Control, 1-13
 - to use WLS Admin server, 1-13
 - to use WLST, 1-13
- Personalization
 - about, 20-1
 - Activity Graph provider, 20-4
 - CMIS provider, 20-4
 - configuration options, 20-4
 - configuration requirements, 20-3
 - configuring Content Presenter, 20-17
 - configuring custom providers, 20-15
 - configuring providers, 20-7
 - configuring single sign-on, 20-20
 - configuring the Activity Graph provider, 20-12
 - configuring the CMIS provider, 20-11
 - installation requirements, 20-3
 - limitations, 20-4
 - managing, 20-1
 - modifying provider connection settings, 20-8
 - OPSS Trust Service, 20-5
 - out-of-the-box configuration, 20-4
 - overriding default security settings, 20-21
 - People Connections locator, 20-5, 20-13
 - prerequisites, 20-2
 - security, 20-3
- policy and credential store, 30-1
- policy store
 - configuring for OID, 30-1
 - exporting and importing, 39-12
- Polls service, performance metrics, 38-36
- portalTools application, 1-8, 8-2
- Portlet Instance Response Time (analytics task flow), 13-3
- Portlet Instance Traffic (analytics task flow), 13-3
- portlet producers
 - about, 24-1
 - considerations, 24-1
 - converting EAR files, 24-17
 - deleting connections
 - in Framework applications, 24-16
 - in WebCenter Portal: Spaces, 24-16
 - using Fusion Middleware Control, 24-15
 - using WLST, 24-15
 - deploying applications, 24-16
 - editing connections
 - using Fusion Middleware Control, 24-13
 - using WLST, 24-14
 - managing post deployment
 - Framework applications, 6-6
 - Spaces application, 6-3
 - managing security, 35-1
 - performance issues and actions, 38-42
 - performance metrics, 38-29
 - registering pagelet producers
 - using Fusion Middleware Control, 25-4

- using WLST, 25-5
- registering PDK-Java producers
 - in Framework applications, 24-12
 - in WebCenter Portal: Spaces, 24-12
 - using Fusion Middleware Control, 24-10
 - using WLST, 24-12
- registering WSRP producers
 - in Framework applications, 24-9
 - in WebCenter Portal: Spaces, 24-9
 - using Fusion Middleware Control, 24-3
 - using WLST, 24-8
- troubleshooting, 24-23
- Portlet Response Time (analytics task flow), 13-3
- Portlet Traffic (analytics task flow), 13-3
- portlets
 - cache size, A-10
 - locale support, A-10
 - performance metrics, 38-31
 - timeouts, A-10
 - tuning performance, A-10
- POST authentication method, 26-6
- Profile service, 18-2
- providers
 - configuring, 20-7
 - configuring custom providers, 20-15
 - modifying provider connection settings, 20-8
- proxy server, 27-2
- public credentials (external applications), 26-7

Q

- QRPPs (Query Result Post-Processors), 12-3

R

- Rank Engine, 12-8
- RCU (Repository Creation Utility), 7-5
- reason strings, customizing, 12-10
- reassociating the policy and credential store, 30-1
- Recent Activities service, performance metrics, 38-38
- Recent History metrics, 38-2
- recipe, 12-3
- redeployment
 - about, 7-28
 - using Fusion Middleware Control, 7-30
 - using WLST, 7-34
 - WebCenter Portal applications, 7-1, 7-27
- refreshGroupSpaceCache (WLST command), 39-73
- refreshSpaceTemplateCache (WLST command), 39-73
- registerPDKJavaProducer (WLST command), 24-12
- registerWSRPProducer (WLST command), 24-8
- Remote Portlet Communication Error, with
 - WebCenter Services Portlets, 24-23
- removeExtAppCredential (WLST command), 26-9
- removeExtAppField (WLST command), 26-9
- removeWorklistConnection (WLST command), 23-14
- renameAGAction (WLST command), 12-13
- renameAGNodeClass (WLST command), 12-13

- Repository Creation Utility (RCU), 7-5
 - ResourceLimitException issue, 39-73
 - resources
 - about, 36-19
 - copying, 36-28
 - creating, 36-27
 - deleting, 36-37
 - downloading, 36-36
 - editing
 - simple editing using Edit dialog, 36-29
 - source code editing, 36-28
 - exporting resources
 - Framework applications, 39-44
 - WebCenter Portal: Spaces, 39-39
 - importing resources
 - Framework applications, 39-44
 - WebCenter Portal: Spaces, 39-40
 - pages
 - access methods, 36-22
 - creating a page, 36-20
 - creating a sub page, 36-22
 - moving pages in page hierarchy, 36-26
 - permission actions, 36-22
 - reordering, 36-25
 - setting access on a page, 36-23
 - setting access on root node, 36-25
 - previewing, 36-36
 - securing, 36-34
 - setting properties
 - associating an icon, 36-32
 - associating attributes, 36-32
 - deleting attributes, 36-33
 - renaming, 36-31
 - showing or hiding, 36-33
 - uploading, 36-36
 - REST APIs, 27-1
 - REST Service Identity Asserter, 29-49
 - REST services
 - about, 27-1
 - authentication, 27-4
 - compression of, 27-4
 - configuring the identity asserter, 29-49
 - managing, 27-1
 - manual configurations, 27-2
 - proxy server configuration, 27-2
 - root name, changing, 27-4
 - security tokens, 27-2
 - reverse proxy
 - rich text editor
 - WebCenter Services Portlets, 24-21
 - roles
 - Framework application roles, 36-6
 - WebLogic Server administrative roles, 1-13
 - roles and responsibilities, 2-1, 2-2, 3-1, 3-2, 4-1, 5-1
 - RSS service
 - about, 21-1
 - performance issues and actions, 38-43
 - performance metrics, 38-37
 - prerequisites, 21-1
 - setting up proxy server
 - using Fusion Middleware Control, 9-5
 - using WLST, 9-5
 - testing a connection, 21-2
 - tuning performance, A-10
 - RTC Web service, 16-2
- ## S
-
- SAML SSO
 - configuring for Framework applications, 32-7
 - SAML-based single sign-on, 31-50
 - Search Metrics (analytics task flow), 13-3
 - Search service
 - connection
 - activating, 22-13
 - creating, 22-10
 - deleting, 22-16
 - managing, 22-1
 - modifying, 22-14
 - performance issues and actions, 38-43
 - performance metrics, 38-38
 - performance tuning, A-10
 - troubleshooting, 22-66
 - usage reports (analytics), 13-3
 - security
 - ADF security, 28-3
 - default configuration, 28-1, 28-4
 - external LDAP, 28-7
 - identity store, 28-5
 - item level security, 11-8
 - Oracle Platform Security Services, 28-3
 - policy store, 28-5, 30-1
 - portlet producers, 35-1
 - securing PDK-Java producers, 35-6
 - single sign-on, 28-8
 - SSL, 28-8
 - WebCenter Portal applications, 28-3
 - WebCenter Security Framework, 28-3
 - WebCenter Spaces, 28-3
 - WebLogic Server security, 28-4
 - WS-Security, 28-8
 - Security Assertion Markup Language, 31-50, 31-51
 - security tokens, 27-2
 - self-registration by invitation, 30-12
 - session timeout, A-9, A-10
 - setAnalyticsCollectorConfig (WLST command), 13-6
 - setAnalyticsCollectorConnection (WLST command), 13-12
 - setBPELConnection (WLST command), 23-13
 - setDiscussionForumConnection (WLST command), 14-10, 14-12
 - setDocumentsSpacesProperties (WLST command), 11-56
 - setDomainEnv.sh, A-9
 - setExtAppConnection (WLST command), 26-9
 - setExtAppCredential (WLST command), 26-9
 - setExtAppField (WLST command), 26-9
 - setMailConnection (WLST command), 17-15
 - setMailConnectionProperty (WLST command), 17-15

- setIMPConnection (WLST command), 16-22, 16-23
- setIMPConnectionProperty (WLST command), 16-23
- setJCRContentServerConnection (WLST command), 11-49, 11-50
- setJCRFileSystemConnection (WLST command), 11-49, 11-51
- setJCRPortalConnection (WLST command), 11-49, 11-51
- setJCRSharePointConnection (WLST command), 11-36
- setMailConnection (WLST command), 17-12, 17-14
- setPDKJavaProducer (WLST command), 24-14
- setPersonalEventConnection (WLST command), 15-11, 15-12
- setProfileCacheNumberOfObjects (WLST command), 13-12
- setProfileCacheTimeToLive (WLST command), 13-12
- setRssProxyConfig (WLST command), 9-5
- setSearchSESSConfig (WLST command), 22-15
- setSESConnection (WLST command), 22-14, 22-15
- setWSRPPProducer (WLST command), 24-14
- shared credentials (external applications), 26-7
- similarity calculation
 - about, 12-3
 - customizing reason strings, 12-10
- Single sign-on
 - Framework applications, 32-1
- single sign-on
 - about, 28-8
 - BPEL server requirements, 23-7
 - configuring with virtual hosts, 31-79
 - external applications, 26-5
 - Microsoft clients, 31-67
 - OAM for Framework applications, 32-4
 - Oracle Access Manager, 31-2
 - Oracle Single Sign-On (OSSO), 31-37
 - SAML SSO for Framework applications, 32-7
 - SAML-based, 31-50
- SMTP
 - about, 17-1
 - SSL security, 17-8
- SOA Suite, 9-2
- Space Response Time (analytics task flow), 13-4
- Space templates
 - exporting and importing, 39-39
- space templates
 - about export and import, 39-4
 - exporting and importing, 39-38
- Space Traffic (analytics task flow), 13-4
- Spaces
 - about
 - administration pages, 1-14
 - export and import, 39-36, 39-37
 - back-end components, 39-24
 - exporting discussions, 39-25
 - importing discussions, 39-27
 - prerequisites, 39-24
 - performance metrics, 38-44
 - usage report (analytics), 13-4
 - viewing and configuring logs, 38-54
 - workflows, 9-2
 - Spaces administrators, 2-2, 3-2
 - Spaces APIs, 34-52
 - Spaces application
 - about import and export, 39-4
 - export and import, 39-1
 - home page in Fusion Middleware Control, 6-2
 - Spaces applications
 - monitoring performance, 38-1
 - tuning performance, A-10
 - Spaces resources
 - See resources
 - SSL security
 - about, 28-8
 - browser connection to Discussions service, 33-15
 - browser connection to WebCenter Spaces, 33-2
 - IMAP connections, 17-8
 - Oracle HTTP Server to WebCenter Spaces, 33-10
 - SES connections, 22-10
 - SMTP connections, 17-8
 - WebCenter Spaces connection to
 - IMAP/SMTP, 33-35
 - WebCenter Spaces connection to LCS, 33-37
 - WebCenter Spaces connection to LDAP, 33-31
 - WebCenter Spaces connection to OCS, 33-37
 - WebCenter Spaces connection to portlet producers, 33-23
 - WebCenter Spaces connection to SES, 33-36
 - start script, 8-2
 - startApplication (WLST command), 8-4, 8-6
 - startNodeManager.sh, 8-2
 - stopApplication (WLST command), 8-5, 8-7
 - string translation, 37-5
 - subscription workflows (WebCenter Portal: Spaces), 9-2
 - subscriptions and notifications, 19-1 to 19-19
 - activities that trigger messages, 19-3
 - connection types
 - about, 19-8
 - setting with Fusion Middleware Control, 19-11
 - setting with WLST commands, 19-12
 - creating custom notification templates, 19-13
 - overwriting default notification templates, 19-14, 19-17
 - preferences in Spaces, 19-7
 - prerequisites, 19-8
 - configuration, 19-9
 - installation, 19-9
 - limitations, 19-9
 - setting up default preferences, 19-2
 - subscription default settings
 - effect on connections, 19-5
 - effect on feedback, 19-6
 - effect on Message Board, 19-5
 - effect on Spaces management, 19-6
 - testing connections, 19-17
 - troubleshooting, 19-18

system libraries, 1-7, 1-8
system limit, A-9
System MBean Browser, 1-20, A-8

T

timeouts
 concurrency management, A-9
 HTTP session, A-9, A-10
 JSP page, A-9
 portlets, A-10
 services and portlets, A-10
translations
 default strings, 37-5
 new languages, 37-7
trans-unit block, 37-6, 37-8
troubleshooting
 Activity Graph service, 12-16
 Analytics service, 13-14
 Discussions and Announcements, 14-17
 Events service, 15-14
 Mail service, 17-18
 Oracle SES search, 22-66
 pagelets, 25-30
 portlet producers, 24-23
 Spaces export and import, 39-72
 subscriptions and notifications, 19-18
 WebCenter Portal application
 configuration, A-10
 WebCenter Services Portlets, 24-21
 WLST commands, A-13
 Worklist service, 23-15
Trust Service, 20-5
 configuring, 20-5, 29-49
 configuring cross-domain trust, 20-7
tuning performance
 Announcements service, A-10
 Discussions service, A-10
 IMP service, A-10
 Mail service, A-10
 Omniportlet producers, A-10
 PDK-Java producers, A-10
 portlets, A-10
 RSS service, A-10
 Search service, A-10
 WSRP producers, A-10

U

undeploying WebCenter Portal applications, 7-25
undeployment
 using Fusion Middleware Control, 7-25
 using WLST, 7-25
 WebCenter Portal applications, 7-1, 7-25
unsetRssProxyConfig (WLST command), 9-6
UPLOAD_MAX_DISK_SPACE parameter, A-5
UPLOAD_MAX_MEMORY parameter, A-5
UPLOAD_TEMP_DIR parameter, A-5
uploadedFileMaxDiskSpace property (Spaces application), A-6

user interface string translation, 37-5
user preferences
 WebCenter Services Portlets, 24-22
user-defined roles (Framework applications), 36-7
users (Framework applications)
 adding and removing, 36-14
 assigning to roles, 36-11
 changing role assignments, 36-13
 granting administrator role, 36-14
 managing, 36-11
 revoking roles, 36-14
users (WebCenter Spaces)
 managing, 30-12

V

virtual hosts, 31-79

W

WC_Collaboration (managed server), 1-7
WC_Custom-diagnostic.log, 38-54
WC_Portlet (managed server), 1-7
WC_Spaces (managed server), 1-7
WC_Spaces-diagnostic.log, 38-54
WC_Uilities (managed server), 1-7
wcSessionTimeoutPeriod, A-6
Web Clipping, 1-8, 8-2, 24-1
webcenter (J2EE application), 1-7, 8-2
WebCenter Portal
 Spaces
 logs, 38-55
 monitoring performance, 38-48
WebCenter Portal applications
 about, 1-12
 administering applications (checklist), 5-1
 configuration changes, A-8
 configuration tools, A-8
 default security, 28-1, 28-4
 deploying, 7-1, 7-12
 identity store, 28-5
 policy store, 28-5
 security, 28-2, 28-3
 See also WebCenter Portal applications
 single sign-on, 31-2
 tuning performance, A-9
 undeploying, 7-25
WebCenter Portal services
 back-end component requirements
 Worklist service, 23-6
 People Connections service
 Activity Stream, 18-2
 setting up connections, 13-1, 23-1
WebCenter Portal Traffic (analytics task flow), 13-3
WebCenter Portal: Framework
 See Oracle WebCenter Portal: Framework
WebCenter Portal: Services, 1-4
WebCenter Portal: Spaces
 about, 1-4
 administering applications (checklist), 3-1

- export and import
 - exporting a space, 39-36
 - exporting a space template, 39-38
 - exporting documents, 39-29
 - importing a space, 39-37
 - importing a space template, 39-39
 - importing documents, 39-29
- See Spaces
- starting and restarting
 - using Fusion Middleware Control, 8-4
 - using WLST, 8-4
- stopping
 - using Fusion Middleware Control, 8-5
 - using WLST, 8-5
- WebCenter Portal's discussions server
 - See discussions server
- WebCenter services
 - database connection, 10-1
 - managing, 10-1
 - setting up connections, 14-1, 15-1, 21-1
- WebCenter Services Portlets, 24-18
 - configuration
 - Announcements service, 24-20
 - Discussions service, 24-20
 - Documents service, 24-19
 - Mail service, 24-20
 - security, 24-21
 - Worklist service, 24-20
 - Lists service permissions, 24-22
 - portlets, 24-18
 - Remote Portlet Communication Error, 24-23
 - rich text editor, 24-21
 - troubleshooting, 24-21
 - user preferences, 24-22
- WebCenter Spaces
 - configuring WS-Security, 34-1
 - granting the administrator role, 30-6
 - security, 28-2, 28-3
- webcenter-config.xml, A-6, A-10
- webcenter-help application, 1-7, 8-2
- WebLogic Administration Console
 - See WebLogic Server Administration Console
- WebLogic Managed Server
 - creating, 7-4
 - provisioning, 7-4
- WebLogic Scripting Tool
 - See WLST
- WebLogic Server Administration Console
 - about, 1-17
 - deploying Portlet Producer applications, 24-18
 - operation summary, 1-14
 - topology, 1-6
- WebLogic Server security, 28-4
- web.xml, A-1, A-5, A-9
- Wiki Metrics (analytics task flow), 13-3
- WLS Administration Console
 - deploying WebCenter Portal applications, 7-21
 - See WebLogic Server Administration Console
- WLST
 - about, 1-18
 - addWorklistConnection, 23-12
 - changing content repository active connection, 11-49
 - createBPELConnection, 23-11
 - createIMPConnection, 16-21
 - createJCRContentServerConnection, 11-48
 - createJCRFileSystemConnection, 11-48
 - createJCRPortalConnection, 11-48
 - createMailConnection, 17-12
 - createPersonalEventConnection, 15-10
 - createSESSConnection, 22-12
 - createSharePointConnection, 11-36
 - deleteAGAction, 12-12
 - deleteAGNodeClass, 12-12
 - deleteAGProviderAssignment, 12-12
 - deleteAGQRPPRegistration, 12-12
 - deleteAGRANKCalculation, 12-12
 - deleteAGSimilarityCalculation, 12-12
 - deleteAllAGMetadata, 12-12
 - deleteConnection, 11-55, 14-13, 15-13, 16-24, 17-17, 22-16, 23-14, 26-10
 - deleteDocumentsSpacesProperties, 11-56
 - deleting content repository connections, 11-55
 - deleting portlet producer connections, 24-15
 - deploying Portlet Producer applications, 24-18
 - deploying WebCenter Portal applications, 7-19
 - editing portlet producer connection details, 24-14
 - exportAGMetadata, 12-11
 - exportAGProviderConfiguration, 12-12
 - exporting a space, 39-36
 - exporting a space template, 39-38
 - exporting portlet client metadata, 39-43
 - exporting resources, 39-39, 39-44
 - exporting Spaces, 39-73
 - exporting WebCenter Portal Spaces, 39-22
 - exporting WebCenter Portal services metadata and data, 39-45
 - exportMetadata command, A-2
 - exportPortletClientMetadata, 24-14
 - getRssProxyConfig, 9-6
 - importAGMetadata, 12-12
 - importing a space, 39-37
 - importing a space template, 39-39
 - importing portlet client metadata, 39-43
 - importing resources, 39-40, 39-41
 - importing WebCenter Portal Spaces, 39-24
 - importing WebCenter Portal service metadata and data, 39-47
 - importPortletClientMetadata, 24-14
 - listDocumentsSpacesProperties, 11-56
 - listSharePointConnection, 11-36
 - managing content repository connection properties (WebCenter Spaces), 11-56
 - migrating Framework application security policies, 39-48
 - modifying content repository connection details, 11-50
 - operation summary, 1-14

- redeploying WebCenter Portal applications, 7-34
- registering an MDS schema, 7-11
- registering content repositories, 11-48
- registering pagelet producers, 25-5
- registering PDK-Java producers, 24-12
- registering WSRP producers, 24-8
- registerPDKJavaProducer, 24-12
- registerWSRPProducer, 24-8
- removeExtAppCredential, 26-9
- removeExtAppField, 26-9
- removeWorklistConnection, 23-12, 23-14
- renameAGAction, 12-13
- renameAGNodeClass, 12-13
- running, 1-18
- setAnalyticsCollectorConnection, 13-12
- setBPELConnection, 23-13
- setDiscussionForumConnection, 14-10, 14-12
- setDocumentsSpacesProperties, 11-56
- setExtAppConnection, 26-9
- setExtAppCredential, 26-9
- setExtAppField, 26-9
- setIMPConnection, 16-22, 16-23
- setIMPConnectionProperty, 16-23
- setJCRContentServerConnection, 11-49, 11-50
- setJCRFileSystemConnection, 11-49, 11-51
- setJCRPortalConnection, 11-49, 11-51
- setMailConnection, 17-12, 17-14, 17-15
- setMailConnectionProperty, 17-15
- setPDKJavaProducer, 24-14
- setPersonalEventConnection, 15-11, 15-12
- setProfileCacheNumberOfObjects, 13-12
- setProfileCacheTimeToLive, 13-12
- setRssProxyConfig, 9-5
- setSearchSESSConfig, 22-15
- setSESSConnection, 22-14, 22-15
- setSharePointConnection, 11-36
- setWSRPProducer, 24-14
- startApplication, 8-4
- stopApplication, 8-5
- undeploying WebCenter Portal applications, 7-25
- unsetRssProxyConfig, 9-6
- wlst.sh script, 1-18
- workflows (WebCenter Portal: Spaces), 9-2
- Worklist service
 - back-end requirements, 23-6
 - configuring for WebCenter Services
 - Portlets, 24-20
 - connection
 - activating, 23-11
 - managing, 23-5
 - modifying, 23-12
 - performance metrics, 38-10
 - Spaces workflows, 9-2
 - troubleshooting, 23-15
- wsm-pm application, 1-8
- WSRP producers
 - performance tuning, A-10
 - registering
 - in Framework applications, 24-9
 - in WebCenter Portal: Spaces, 24-9
 - using Fusion Middleware Control, 24-3
 - using WLST, 24-8
 - testing connections, 24-9
 - WS-Security, 35-1
- wsrp-tools application, 1-8, 8-2
- WS-Security
 - about, 28-8
 - BPEL server, 23-7
 - configuring, 34-1
 - configuring for a complex topology, 34-23
 - configuring for a simple topology, 34-1
 - configuring for a typical topology, 34-13
 - discussions server, 14-4
 - Spaces APIs, 34-52
 - WSRP producers, 35-1